FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1349901-0

Total Deleted Page(s) = 212
Page 16 ~ b7E;
Page 17 ~ b7E;
Page 18 ~ b7E;
Page 19 ~ b7E;
Page 23 ~ b7E;
Page 24 ~ b7E;
Page 25 ~ b7E;
Page 26 ~ b7E;
Page 27 ~ b7E;
Page 32 ~ b7E;
Page 33 ~ b7E;
Page 34 ~ b7E;
Page 35 ~ b7E;
Page 36 ~ b7E;
Page 37 ~ b7E;
Page 41 ~ b7E;
Page 42 ~ b7E;
Page 45 ~ b7E;
Page 48 ~ b7E;
Page 51 ~ b7E;
Page 56 ~ b7E;
Page 65 ~ Duplicate;
Page 80 ~ Duplicate;
Page 81 ~ Duplicate;
Page 82 ~ Duplicate;
Page 83 ~ Duplicate;
Page 84 ~ Duplicate;
Page 85 ~ Duplicate;
Page 86 ~ Duplicate;
Page 90 ~ Duplicate;
Page 94 ~ b7E;
Page 96 ~ b7E;
Page 99 ~ Duplicate;
Page 112 ~ b7E;
Page 130 ~ Duplicate;
Page 137 ~ b7E;
Page 139 ~ Duplicate;
Page 141 ~ Duplicate;
Page 142 ~ Duplicate;
Page 143 ~ Duplicate;
Page 154 ~ b7E;
Page 155 ~ b7E;
Page 156 ~ b7E;
Page 157 ~ b7E;
Page 158 ~ b7E;
Page 159 ~ b7E;
Page 160 ~ b7E;
Page 161 ~ b7E;

Page 162 ~ b7E;
Page 163 ~ b7E;
Page 164 ~ b7E;
Page 165 ~ b7E;
Page 166 ~ b7E;
Page 167 ~ b7E;
Page 168 ~ b7E;
Page 169 ~ b7E;
Page 170 ~ b7E;
Page 171 ~ b7E;
Page 172 ~ b7E;
Page 173 ~ b7E;
Page 174 ~ b7E;
Page 175 ~ b7E;
Page 176 ~ b7E;
Page 177 ~ b7E;
Page 178 ~ b7E;
Page 179 ~ b7E;
Page 180 ~ b7E;
Page 181 ~ b7E;
Page 182 ~ b7E;
Page 183 ~ b7E;
Page 184 ~ b7E;
Page 185 ~ b7E;
Page 186 ~ b7E;
Page 187 ~ b7E;
Page 188 ~ b7E;
Page 189 ~ b7E;
Page 190 ~ b7E;
Page 191 ~ b7E;
Page 192 ~ b7E;
Page 193 ~ b7E;
Page 194 ~ b7E;
Page 195 ~ b7E;
Page 196 ~ b7E;
Page 197 ~ b7E;
Page 198 ~ b7E;
Page 199 ~ b7E;
Page 202 ~ b7E;
Page 203 ~ b7E;
Page 204 ~ b7E;
Page 205 ~ b7E;
Page 206 ~ b7E;
Page 207 ~ b7E;
Page 208 ~ b7E;
Page 209 ~ b7E;
Page 210 ~ b7E;
Page 211 ~ b7E;
Page 212 ~ b7E;
Page 213 ~ b7E;
Page 214 ~ b7E;
Page 215 ~ b7E;
Page 216 ~ b7E;
Page 217 ~ b7E;

Page 218 ~ b7E;
Page 219 ~ b7E;
Page 220 ~ b7E;
Page 221 ~ b7E;
Page 222 ~ b7E;
Page 223 ~ b7E;
Page 224 ~ b7E;
Page 225 ~ b7E;
Page 226 ~ b7E;
Page 227 ~ b7E;
Page 228 ~ b7E;
Page 229 ~ b7E;
Page 230 ~ b7E;
Page 231 ~ b7E;
Page 232 ~ b7E;
Page 233 ~ b7E;
Page 234 ~ b7E;
Page 235 ~ b7E;
Page 236 ~ b7E;
Page 237 ~ b7E;
Page 238 ~ b7E;
Page 239 ~ b7E;
Page 240 ~ b7E;
Page 241 ~ b7E;
Page 278 ~ b7E;
Page 279 ~ b7E;
Page 280 ~ b7E;
Page 286 ~ b7E;
Page 287 ~ b7E;
Page 288 ~ b7E;
Page 289 ~ b7E;
Page 290 ~ b7E;
Page 291 ~ b7E;
Page 293 ~ b7E;
Page 294 ~ b7E;
Page 295 ~ b7E;
Page 296 ~ b7E;
Page 297 ~ b7E;
Page 300 ~ b7E;
Page 301 ~ b7E;
Page 302 ~ b7E;
Page 303 ~ b7E;
Page 304 ~ b7E;
Page 305 ~ b7E;
Page 306 ~ b7E;
Page 307 ~ b7E;
Page 308 ~ b7E;
Page 309 ~ b7E;
Page 310 ~ b7E;
Page 311 ~ b7E;
Page 312 ~ b7E;
Page 313 ~ b7E;
Page 314 ~ b7E;
Page 315 ~ b7E;

Page 316 ~ b7E;
Page 318 ~ b7E;
Page 321 ~ b7E;
Page 322 ~ b7E;
Page 324 ~ b7E;
Page 325 ~ b7E;
Page 326 ~ b7E;
Page 327 ~ b7E;
Page 328 ~ b7E;
Page 329 ~ b7E;
Page 330 ~ b7E;
Page 331 ~ b7E;
Page 333 ~ b7E;
Page 334 ~ b7E;
Page 335 ~ b7E;
Page 336 ~ b7E;
Page 340 ~ b7E;
Page 341 ~ b7E;
Page 342 ~ Duplicate;
Page 343 ~ Duplicate;
Page 344 ~ Duplicate;
Page 345 ~ Duplicate;
Page 346 ~ Duplicate;
Page 347 ~ Duplicate;
Page 348 ~ Duplicate;
Page 349 ~ Duplicate;
Page 350 ~ Duplicate;
Page 351 ~ Duplicate;
Page 352 ~ Duplicate;
Page 353 ~ Duplicate;
Page 354 ~ Duplicate;
Page 355 ~ Duplicate;
Page 356 ~ Duplicate;
Page 357 ~ Duplicate;
Page 358 ~ Duplicate;
Page 359 ~ Duplicate;
Page 360 ~ Duplicate;
Page 361 ~ Duplicate;
Page 362 ~ Duplicate;
Page 363 ~ Duplicate;
Page 364 ~ Duplicate;
Page 365 ~ Duplicate;
Page 366 ~ Duplicate;
Page 367 ~ Duplicate;
Page 368 ~ Duplicate;
Page 369 ~ Duplicate;
Page 370 ~ Duplicate;
Page 371 ~ Duplicate;
Page 372 ~ Duplicate;
Page 373 ~ Duplicate;
Page 374 ~ Duplicate;
Page 375 ~ Duplicate;
Page 376 ~ Duplicate;
Page 377 ~ Duplicate;

Page 378 ~ Duplicate;
Page 379 ~ Duplicate;

```
XXXXXXXXXXXXXXXXXXXXXXXX
X   Deleted Page(s)    X
X   No Duplication Fee X
X   For this Page      X
XXXXXXXXXXXXXXXXXXXXXXXX
```

Loading Social Media for Law Enforcement: Friend or Foe
Please Wait ...

Course Summary

What did this course cover?

This course explored social media tools available to you throughout an investigation. Through the scenario, you learned how to continue a search after hitting road-blocks using common search engines such as Google or Bing; [redacted] b7E and how to find useful information through content that subjects post and make public on social media sites.

Now that you've completed this course, you should be able to:

1. Explain the unique advantages of using different social media sites [redacted] b7E
2. Perform [redacted] for investigative purposes on social media sites [redacted]
3. Explain proper procedures for conducting social media searches

UNCLASSIFIED

Exit

Glossary
Printer
Guidelines
Tools and Capabilities

Previous
Next
Page

Course Summary

UNCLASSIFIED

Exit

Glossary
Printer
Guidelines
Tools and Capabilities

Previous
Next
Page

More Investigative Technology Courses and FYIs

If you want to learn more about HiTET, check out these additional resources on FBINet's Virtual Academy.

Courses:

- Basic Networking for Investigators for Law Enforcement
- Exploiting Mobile Communications for Law Enforcement: Criminal Tactics and Investigative Techniques
- Obtaining and Analyzing Digital Records for Law Enforcement
- The Cloud for Law Enforcement: It's All About Communication
- Investigating Websites for Law Enforcement: A Wealth of Information
- Tracing Email Addresses for Law Enforcement

FYIs

- Email Draft Folder Messaging Podcast
- File Hashing
- Using Public Records Databases in Investigations
- Virtual Worlds

For more information on each click here.

Course Summary

References, Job Aids and Tools

Still have questions?

If you need more in-depth expertise on this topic, please contact technical experts in your area.

References

UNCLASSIFIED

Exit

Glossary
Printer
Guidelines
Tools and Capabilities

Previous

Next

Page

Before you exit the course, print or save the entire course content and/or job aids for reference by clicking on each link

- Social Media For Law Enforcement: Friend or Foe - text only

- Social Media Guidelines for Law Enforcement
- Social Sites Capabilities

The following references were used to develop the content of this course:

- [redacted]

b7E

Course Summary

Conclusion

Exit

Glossary
Printer
Guidelines
Tools and Capabilities

Previous
Page
Next

You have completed the "Course Summary."

Select Next to continue to the Post-test.

Getting Started

This course includes audio, video, and multimedia animations that require Flash Player 10 or higher. To ensure proper functionality of this course, please:

- Ensure your computer is running Adobe Flash Player version 10 or higher. To upgrade your Adobe Flash Player, contact the IT Support Desk.
- Clear your browser history.
- Press SHIFT + CTRL + DELETE on your keyboard.
- Select all checkboxes except "Preserve Favorites Website Data" and click on the Delete button.
- Close out any additional windows and programs that you have open.
- Make sure your speakers are turned on or a head set is plugged in.

UNCLASSIFIED

Exit

Next

Page

Getting Started

Welcome to "Social Media for Law Enforcement: Friend or Foe."

This course familiarizes investigators with some of the social media tools available to them throughout an investigation. Key topics covered in this course are: how to search for individual accounts using [redacted] how to find [redacted] and how to find useful public content on social media sites for investigations. b7E

Why is this course important to investigators?

There is a substantial amount of valuable information available through social media, but you would have to know where to go and how to search for it. By applying the techniques and by using the tools presented in this course, you will gain yet another path of useful leads in an investigation.

This Investigative Technology Training course maximizes investigative capabilities by advancing the core technical skills for investigators. Investigative Technology Training enables these individuals to increase their ability to apply technology in investigations and intelligence matters.

UNCLASSIFIED
Exit
Next
Page

Getting Started

This course places you in an interactive environment in which you will receive immediate feedback based on the choices you make throughout the course to solve the given case. Every module will introduce new material and provide an update on the current phase of the investigation. At the end of each module, you will use the given information to contribute in each step of the investigation until in the end the case is solved!

UNCLASSIFIED

Exit
Next Page

Getting Started

UNCLASSIFIED

Exit
Next
Page

Course Instructional Goal and Learning Objectives

The goal of this course is to illustrate how investigators can utilize social media, consistent with policy, to further their investigations.

After completing this course, investigators will be able to:

1. Explain the unique advantages of using different social media sites [redacted] b7E
2. Perform [redacted] for investigative purposes on social media sites [redacted] [redacted]
3. Explain proper procedures for conducting social media searches

Getting Started

Exit
Next
Page

DISCLAIMER

This course features a job aid that includes social media sites investigators can use consistent with policy to help with their investigations. However, the sites introduced in this course are not all-inclusive. Please note there are many more available through the internet.

IMPORTANT: Please remember the sensitivity and legal requirements of using social media. Please contact your state or local prosecuting attorney for further guidance.

Getting Started

UNCLASSIFIED

Exit

Next

Page

About this course: Organization, Job Aids, Post-test

Organization

This course is divided into three lessons and a summary.

- Lesson 1: What's In a Username
- Lesson 2: Strategic Social Searches
- Lesson 3: Tale-telling [redacted]

b7E

Job Aids

This course is designed to encourage the use of the job aids (available after completing Getting Started) to complete some of the learning activities. There are two job aids in this course, which are also available as stand-alone references in the unclassified Virtual Academy.

- Social Media Guidelines for Law Enforcement
- Social Sites Capabilities

Post-test

There is a test at the end of the course to assess your learning. You must achieve a score of at least 80% on this post-test to receive credit for completion.

Other Features

Investigative Notes

As your investigation unfolds, any helpful facts that you come across will be displayed in your investigative notes.

Glossary

For a printable version of the glossary , which contains definitions of key terms used throughout the course, click on the "glossary" link located at the bottom of each page that will appear beginning in lesson 1.

Printable Version

A printable version of the course is available for you to print or save the content of this course for future reference. It can also be useful while taking the course, for taking notes or highlighting points that you find most useful.   This version will be accessible by clicking on the printer link located at the bottom of each page that will appear beginning in lesson 1.

Getting Started

You have completed "Getting Started".

Click Next to continue to "Lesson 1: Types of Information and Providers."

UNCLASSIFIED

Exit

Next

Page

Conclusion

Pre-Test Option

You have completed "Getting Started"

This course features a pre-test option. If you feel that you already possess expertise on this topic, you can attempt the pre-test and opt out of the course. You must achieve a score of 100% on this pre-test to receive credit for completion.

Note: This is your only chance to take this pre-test. If you continue with the course, you will not be able to come back and take the pre-test later.

If you wish to attempt the pre-test click here or click Next to continue to "Lesson 1: What's in a Username."

Next

Lesson 1: What's In a User-Name

Introduction

This lesson will introduce you to the case you will be investigating during the course. You will learn about the information already gathered and the investigative work already conducted.

You will be introduced to [redacted] a couple of tools that can be more useful than Google or Bing when searching social media sites. b7E

After completing this lesson, you will be able to:

- Perform a search on [redacted]
- Explain the advantages of using [redacted] over Google or Bing
- Identify the benefits of using [redacted]

UNCLASSIFIED

Exit

Glossary
Printer
Guidelines
Tools and Capabilities

Previous
Next
Page

Lesson 1: What's In a User-Name

UNCLASSIFIED

Exit

Glossary

Printer

Guidelines

Tools and Capabilities

Previous

Next

Page

[redacted]

b7E

Check your answer!

Lesson 1: What's In a User-Name

Lesson Conclusion

UNCLASSIFIED

Exit

Glossary

Printer

Guidelines

Tools and Capabilities

Previous

Next

Page

You have completed reviewing "Lesson 1: What's In a User-Name".

Select the next button to review "Lesson 2: Strategic Social Searches."

You have completed "Lesson 1: What's in a User-Name."

This lesson introduced you to the case you will be investigating during the course. You learned about the information already gathered and to the investigative work already conducted.

You were introduced to [redacted] a tool that is more useful than Google or Bing when searching social media sites. b7E

Now that you have completed this lesson, you should be able to:

- Perform a search on [redacted]
- Explain the advantages of using [redacted] over Google or Bing
- Identify the benefits of using [redacted]

Select Next to continue to "Lesson 2: Strategic Social Searches."

Lesson 1: What's In a User-Name

This investigation is fictitious in nature and is not designed to teach investigative strategies. The purpose of this course is to provide an interactive and stimulating vehicle to raise awareness of social media sites and their potential benefits in an investigation

Lesson 1: What's In a User-Name

UNCLASSIFIED

Exit

Glossary

Printer

Guidelines

Tools and Capabilities

Previous

Next

Page

[redacted]

b7E

Click on the key word links to learn more.

Lesson 1: What's In a User-Name

UNCLASSIFIED

Exit

Glossary

Printer

Guidelines

Tools and Capabilities

Previous

Next

Page

[redacted]

b7E

Check your answer!

Lesson 2: Strategic Social Searches

Introduction

This This lesson explores the steps that you would need to perform searches on [redacted] and to search [redacted]

b7E

After completing this lesson, you will be able to:

- Perform searches on [redacted]
- View and interpret results displayed on [redacted]
- Use a [redacted]
- Navigate through [redacted]

UNCLASSIFIED

Exit

Glossary
Printer
Guidelines
Tools and Capabilities

Previous
Next
Page

Lesson 2: Strategic Social Searches

Conclusion

UNCLASSIFIED

Exit

Glossary
Printer
Guidelines
Tools and Capabilities

Previous
Next
Page

You have completed reviewing "Lesson 2: Strategic Social Searches."

Select Next to continue to "Lesson 3: Tale-Telling [redacted] '

Next

You have completed "Lesson 2: Strategic Social Searches."

This lesson explored the steps that you would need to perform searches on [redacted] and to search [redacted] b7E
[redacted]

Now that you've completed this lesson you:

- Performed searches on [redacted]
- Viewed and interpreted results displayed on [redacted]
- Used a [redacted]
- Navigated through [redacted]

Select Next to continue to "Lesson 3: Tale-Telling [redacted] '

Next

Lesson 2: Strategic Social Searches

UNCLASSIFIED

Exit

Glossary

Printer

Guidelines

Tools and Capabilities

Previous

Next

Page

[redacted]

b7E

Check your answer!

Lesson 2: Strategic Social Searches

When it comes to social sites, despite an individual's efforts to keep their information private, [redacted] b7E

[redacted]

[redacted] b7E

UNCLASSIFIED

Exit

Glossary
Printer
Guidelines
Tools and Capabilities

Previous
Next
Page

Lesson 3: Tale-Telling [redacted]

Introduction

This lesson introduces [redacted] which allows you to search for and view [redacted] based b7E on the given parameters. You will explore the steps needed to perform [redacted]

After completing this lesson, you will be able to:

- Perform [redacted]
- Obtain [redacted] relevant to keywords
- Refine searches on [redacted]

UNCLASSIFIED

Exit

Glossary

Printer

Guidelines

Tools and Capabilities

Previous

Next

Page

Lesson 3: Tale-Telling [redacted]

b7E

[redacted]

IMPORTANT NOTICE:

The U.S. Supreme Court ruled in a unanimous decision in Riley v. California that a search warrant is generally required to search the contents of a cell phone seized on an arrestee, and a warrantless search can no longer be conducted as part of a search incident to arrest exception to the 4th Amendment warrant requirement. Other exceptions to the warrant requirement continue to apply and arresting officers can also obtain the consent of an arrestee to search the contents of a phone without first obtaining a warrant.

UNCLASSIFIED

Exit

Glossary
Printer
Guidelines
Tools and Capabilities

Previous
Next
Page

Lesson 3: Tale-Telling [redacted]

Conclusion

b7E

UNCLASSIFIED

Exit

Glossary

Printer

Guidelines

Tools and Capabilities

Previous Page

You have completed reviewing "Lesson 3: Tale-Telling [redacted]"

Select Next to retake the Post-Test.

Next

You have completed "Lesson 3: Tale-Telling [redacted]"

This lesson introduces [redacted] which allows you to search for and view [redacted] based on the given parameters. You will explore the steps needed to perform [redacted]

b7E

After completing this lesson, you will be able to:

- Perform [redacted]
- Obtair [redacted] relevant to keywords
- Refine searches on [redacted]

Select Next to continue to the Course Summary.

Next

Lesson 3: Tale-Telling [redacted]

b7E

Twitter's is a real-time information network that lets users share and discover what's happening now. Law enforcement must provide Twitter a subpoena for subscriber information.

In case of an emergency situation, an emergency disclosure request to obtain this information more quickly.

It's important to note that most service providers have a policy to notify subscribers when law enforcement serves process for any information. In case of a covert investigation, you must submit a court order for non-disclosure along with a subpoena.

Joining an e-mail list or Twitter feed of an organization is participation that must abide by the policy of your organization. If the general public is not able to sign up to the twitter feed or the e-mail list, then additional approvals may be necessary.

UNCLASSIFIED

Exit

Glossary
Printer
Guidelines
Tools and Capabilities

Previous
Next
Page

Lesson 3: Tale-Telling [redacted]

b7E

Most Twitter profile information is public, so anyone can see it. A Twitter profile contains a profile photo, header photo, background image, and status updates, called tweets. In addition, the user has the option to fill out location, a URL, and a short "bio" section about themselves for display on their public profile.

[redacted]

b7E

[redacted]

b7E

[redacted]

[redacted]

[redacted]

UNCLASSIFIED

Exit

Glossary

Printer

Guidelines

Tools and Capabilities

Previous

Next

Page

Lesson 3: Tale-Telling [redacted]

b7E

UNCLASSIFIED

Exit

Glossary

Printer

Guidelines

Tools and Capabilities

Previous

Next

Page

What do you think

[redacted]

b7E

Check your answer!

Lesson 3: Tale-Telling [redacted]

Remember

Twitter Search can be used to identify tweets containing a word or phrase within a geographic location. These tweets can be helpful to investigators using Twitter to create a stream of relevant information. [redacted] b7E

Also remember that only those Tweets that are pertinent to and within the scope of the case may be collected.

UNCLASSIFIED

Exit

Glossary
Printer
Guidelines
Tools and Capabilities

Previous
Next
Page

Courses

- Basic Networking for Law Enforcement - This course teaches the fundamentals of networking and the Internet as it is relevant to investigations. Key topics covered in this course include: how a device accesses the Internet; the standard devices that make up a network; MAC addresses, using Internet resources to identify registration; ownership of domains and IP addresses; types of network-based investigative information available; how criminals may exploit the capabilities of the Internet, and the common user devices that access the Internet.

- Exploiting Mobile Communications for Law Enforcement: Criminal Tactics and Investigative Techniques - This course familiarizes Special Agents, Intelligence Analysts, and professional staff with the mobile communication technologies they may encounter throughout investigations. Key topics covered in this course are: how mobile communications networks are designed, how criminals use mobile devices, and how investigators can analyze mobile communications to further their investigation and ensure operational security. This course is ~~For Official Use Only/Law Enforcement Sensitive.~~

- Obtaining and Analyzing Digital Records for Law Enforcement - This course explains how to preserve, access, obtain, and analyze digital records in support of an FBI investigation. Key topics covered in this course include: different types of digital information and where to find it, preserving digital evidence, and using digital records in investigations.

- The Cloud for Law Enforcement: It's All About Communication - This course is designed as a familiarization to introduce the basics of Internet cloud storage. This course will focus on the elements of cloud architecture and the various uses of the cloud including: communications, storage, computing, and how they relate to investigations and intelligence gathering. The knowledge gained from this entry level course will be used as the basis for future and existing advanced cloud computing courses.

- Investigating Websites for Law Enforcement: A Wealth of Information - This course will teach investigators about the investigative information that can be obtained from Web sites. Quite a bit of information can be found on a Web site, or embedded within a Web site. Investigators need to know what this information is, how they can access it, and how it can be used in their investigations.

- Tracing Email Addresses - This scenario-based course will explain how to view and analyze an extended email header and how to exploit that information to further your investigations. Key topics covered in this course are: defining email headers; how to display extended email headers; how to identify relevant investigative information contained in the extended header; how to locate the originating Internet protocol (IP) address, date, and time stamp in an email header; and how to trace an IP address.

FYIs

- Email Draft Folder Messaging Podcast - This Podcast describes how Email Draft Folder Messaging works, where you can locate the folder, examples of when it was used, how to identify when suspects are using it, and how to defeat it. This podcast was developed in support of HiTET. This podcast is ~~For Official Use Only/Law Enforcement Sensitive.~~

- File Hashing - This FYI will introduce the learner to file hashing, explore hashing's investigative uses, and demonstrate how to hash

[redacted]

Click to close

Deep Web refers to a vast repository of underlying content, such as documents in online databases that general-purpose web crawlers cannot reach. The deep web content is estimated at 500 times that of the surface web, yet has remained mostly untapped due to the limitations of traditional search engines. Any documents or information found through the deep web will still require investigators to contact the companies in possession of the information and present the required legal documents to acces the information. [redacted] b7E

CLOSE

18.5.1.1 (U) Scope

(U) Published information is “Publicly Available Information” that is:

A) (U) Published or broadcast for public consumption;

B) (U) Available on request to the public;

C) (U) Accessible on-line or otherwise to the public;

D) (U) Available to the public by subscription or purchase;

E) (U) Made available at a meeting open to the public;

F) (U) Obtained by visiting any place or attending an event that is open to the public (e.g., public places); or

G) (U) Observed, heard, smelled, detected or obtained by any casual observer or member of the public and does not involve unconsented intrusion into private places.

Click to close

Post-Test

You have already successfully completed the test for this course. If desired, utilize the side bar menu to browse the lessons you have already completed.
You must achieve a score of at least 80% on this post-test to receive credit for completion of this course.

Important! You must complete the entire post-test before exiting the course. If you only complete a portion of the test, your results will not be saved and you will have to complete the entire test again when you return to the course.

Click Next to continue.

UNCLASSIFIED

Exit

Glossary
Printer
Guidelines
Tools and Capabilities

Next

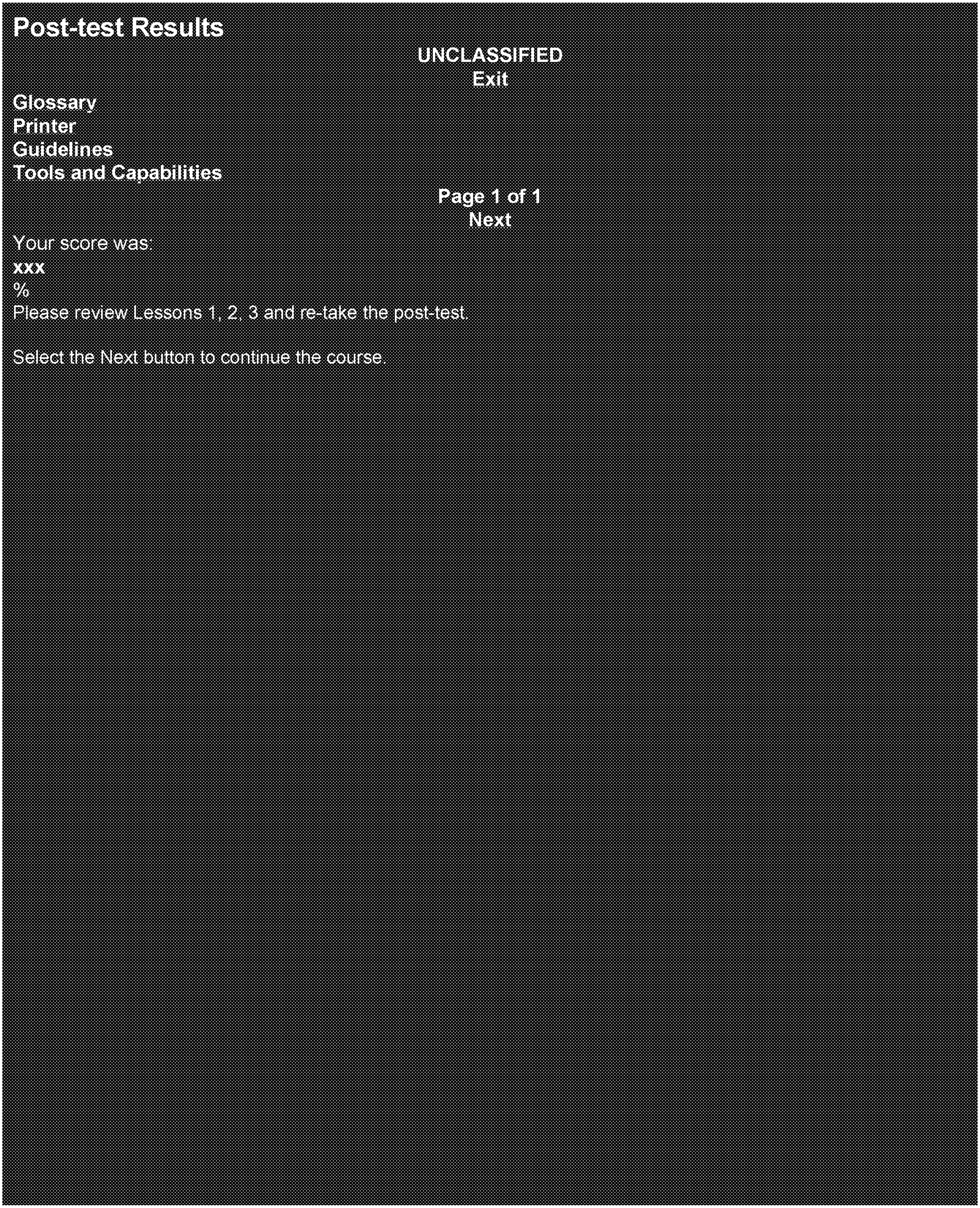
UNCLASSIFIED

Page

Previous

Instructions

Next



Post-test Results

UNCLASSIFIED

Exit

Glossary

Printer

Guidelines

Tools and Capabilities

Page 1 of 1

Next

Your score was:

xxx

%

Please review Lessons 1, 2, 3 and re-take the post-test.

Select the Next button to continue the course.

Post-test Results

xxx

UNCLASSIFIED

Exit

Glossary
Printer
Guidelines
Tools and Capabilities

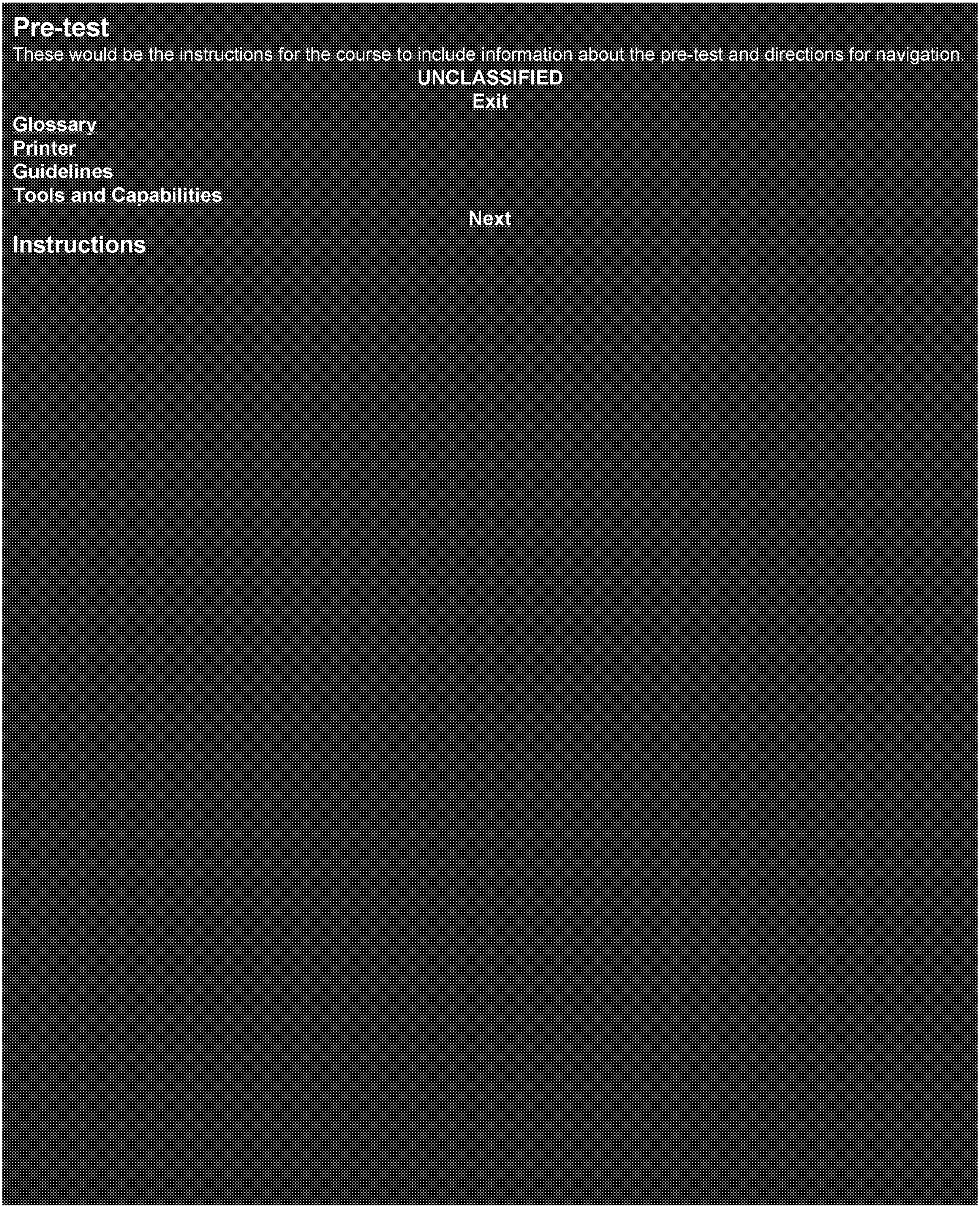
Page 1 of 1

Next

Congratulations! You have passed the post-test for the *Social Media: Friend or Foe* course with a score of .

Select Exit to mark the course completed and to close the course.

%



Pre-test

These would be the instructions for the course to include information about the pre-test and directions for navigation.

UNCLASSIFIED

Exit

Glossary
Printer
Guidelines
Tools and Capabilities

Next

Instructions

Pre-test Results

UNCLASSIFIED
Exit
Page 1 of 1
Next

Your score was:
xxx
%
You need to take the *Social Media: Friend or Foe* course and pass the post-test to successfully complete this course.

Select the Next button to continue the course.

Pre-test Results

xxx

Exit

Glossary

Printer

Guidelines

Tools and Capabilities

Page 1 of 1

Next

Congratulations! You have passed the pre-test for the *Social Media: Friend or Foe* course with a score of .

Click here to complete the survey before exiting this course.

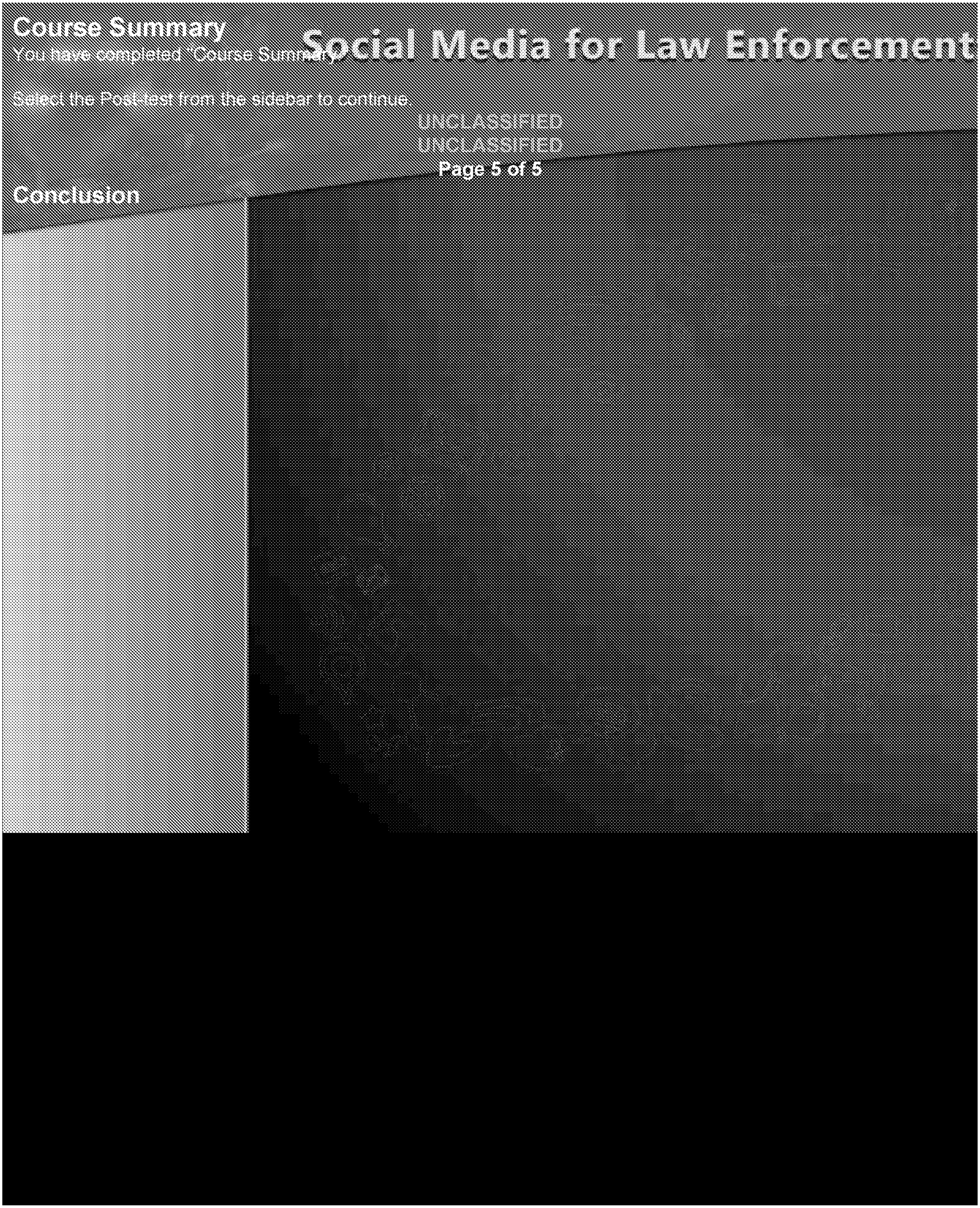
%

Exit

Printer
Guidelines

Next

This course is sponsored by the Training Division.



Course Summary

You have completed "Course Summary"

Social Media for Law Enforcement

Select the Post-test from the sidebar to continue.

Page 5 of 5

Conclusion

Course Summary

More Investigative Technology Courses and FYIs

If you want to learn more about Investigative Technology, check out these additional resources on the Unclassified Virtual Academy.

Roll over each item to see more information.

- Course: Basic Networking for Investigators for Law Enforcement
- Course: Exploring Mobile Communications for Law Enforcement: Criminal Tactics and Investigative Techniques
- Course: Obtaining and Analyzing Digital Records for Law Enforcement
- Course: The Cloud for Law Enforcement: It's All About Communication
- Course: Investigating Websites for Law Enforcement: A Wealth of Information
- Course: Tracing Email Addresses for Law Enforcement
  - FYI: Email Draft Folder Messaging Podcast
  - FYI: File Hashing
  - FYI: Using Public Records Databases in Investigations
  - FYI: Virtual Worlds

VIRTUAL ACADEMY

Course: Tracing Email Addresses

This scenario-based course will explain how to view and analyze an extended email header and how to exploit that information to further your investigations. Key topics covered in this course are: defining email headers; how to display extended email headers; how to identify relevant investigative information contained in the extended header; how to locate the originating Internet protocol (IP) address, date, and time stamp in an email header; and how to trace an IP address.

VIRTUAL ACADEMY

Mobile Open Source Tool (MOST) Google Series

Part 1: Part one of a three part series discusses the effective use of Google Search Operators.

Part 2: Part two of this three part series discusses how to use search results filters effectively.

Part 3: The last of a three part series, this video discusses how to use Google Maps effectively.

VIRTUAL ACADEMY

FYI: Virtual Worlds

This FYI will define virtual worlds and massively multiplayer online role playing games, identify common gamer language, describe ways criminals and terrorists exploit virtual worlds, and describe how investigators can use virtual worlds in their investigations. Virtual worlds are being exploited in different ways by criminals and extremists. Investigators need to be aware of these ways and know how to investigate a subject's involvement in virtual worlds.

VIRTUAL ACADEMY

FYI: Using Public Records Databases in Investigations

This FYI was developed as a job aid for use in your investigations. It shows you the types of information you can get from the many different categories of public records databases. We have an arsenal of tools available to us when we conduct our investigations. One of these tools is the Internet. There is a vast amount of information available through a variety of public records databases.

VIRTUAL ACADEMY

FYI: File Hashing

This FYI will introduce the learner to file hashing, explore hashing's investigative uses, and demonstrate how to hash a file using both online and downloaded file hashing tools. File hashing is a very useful tool for computer forensics. By examining a file hash, investigators can determine if a file has changed, if two files are identical, or differentiate between system operating files and user-generated files. Making these determinations drastically reduces the amount of time needed to review computer files when searching for evidence.

VIRTUAL ACADEMY

FYI: Email Draft Folder Messaging Podcast

This Podcast describes how Email Draft Folder Messaging works, where you can locate the folder, examples of when it was used, how to identify when suspects are using it, and how to defeat it. This podcast was developed in support of HiTET. This podcast is For Official Use Only/Law Enforcement Sensitive.

VIRTUAL ACADEMY

Course: Investigating Websites for Law Enforcement: A Wealth of Information

This course will teach investigators about the investigative information that can be obtained from Web sites. Quite a bit of information can be found on a Web site, or embedded within a Web site. Investigators need to know what this information is, how they can access it, and how it can be used in their investigations.

VIRTUAL ACADEMY

Course: The Cloud for Law Enforcement: It's All About Communication

This course is designed as a familiarization to introduce the basics of Internet cloud storage. This course will focus on the elements of cloud architecture and the various uses of the cloud including: communications, storage, computing, and how they relate to investigations and intelligence gathering. The knowledge gained from this entry level course will be used as the basis for future and existing advanced cloud computing courses.

VIRTUAL ACADEMY

Course: Obtaining and Analyzing Digital Records for Law Enforcement

This course explains how to preserve, access, obtain, and analyze digital records in support of an FBI investigation. Key topics covered in this course include: different types of digital information and where to find it; preserving digital evidence; and using digital records in investigations.

VIRTUAL ACADEMY

Course: Exploiting Mobile Communications for Law Enforcement: Criminal Tactics and Investigative Techniques

This course familiarizes Special Agents, Intelligence Analysts, and professional staff with the mobile communication technologies they may encounter throughout investigations. Key topics covered in this course are: how mobile communications networks are designed, how criminals use mobile devices, and how investigators can analyze mobile communications to further their investigation and ensure operational security. This course is For Official Use Only/Law Enforcement Sensitive.

VIRTUAL ACADEMY

Course: Basic Networking for Law Enforcement

This course teaches the fundamentals of networking and the Internet as it is relevant to investigations. Key topics covered in this course include: how a device accesses the Internet; the standard devices that make up a network; MAC addresses, using Internet resources to identify registration; ownership of domains and IP addresses; types of network-based investigative information available; how criminals may exploit the capabilities of the Internet, and the common user devices that access the Internet.

[redacted]

Course Summary

References, Job Aids and Tools

Still have questions?

If you need more in-depth expertise on this topic, please contact technical experts in your area.

UNCLASSIFIED

UNCLASSIFIED

Page

Before you exit the course, print or save the entire course content and/or job aids for reference.

- Social Media For Law Enforcement: Friend or Foe – text only
- Social Media Guidelines for Law Enforcement
- Social Sites Capabilities

Course Summary
References

Social Media for Law Enforcement

UNCLASSIFIED

UNCLASSIFIED

Page

The following references were used to develop the content of this course.

- [redacted]

b7E

Getting Started
Other Features

Social Media for Law Enforcement

Investigative Notes

As your investigation unfolds, any helpful facts that you come across will be displayed in your investigative notes.

Glossary

For a printable version of the glossary , which contains definitions of key terms used throughout the course, click on the "glossary" icon located at the bottom of each page that will appear beginning in lesson 1.

Printable Version

A printable version of the course is available for you to print or save the content of this course for future reference. It can also be useful while taking the course; for taking notes or highlighting points that you find most useful. This version will be accessible after completing the Getting Started section.

Getting Started

Social Media for Law Enforcement

You have completed "Getting Started."

Select Lesson 1 from the sidebar to continue.

UNCLASSIFIED
UNCLASSIFIED
Page

Pre-test Option

You have completed "Getting Started."

This course features a pre-test option. If you feel that you already possess expertise on this topic, you may attempt the pre- test to opt out of the course. You must achieve a score of 100% on this pre-test to receive credit for completion.

Note: This is your only chance to take this pre-test. If you continue with the course, you will not be able to come back and take the pre-test later.

If you successfully complete the pre-test, all lessons will be unlocked and available for your review, if you wish to review the course content later.

If you wish to attempt the pre-test click the pre-test icon.

Click the complete button () to unlock the next lesson.

Conclusion

Lesson 1: What's In a User-Name

Social Media for Law Enforcement

You have completed "

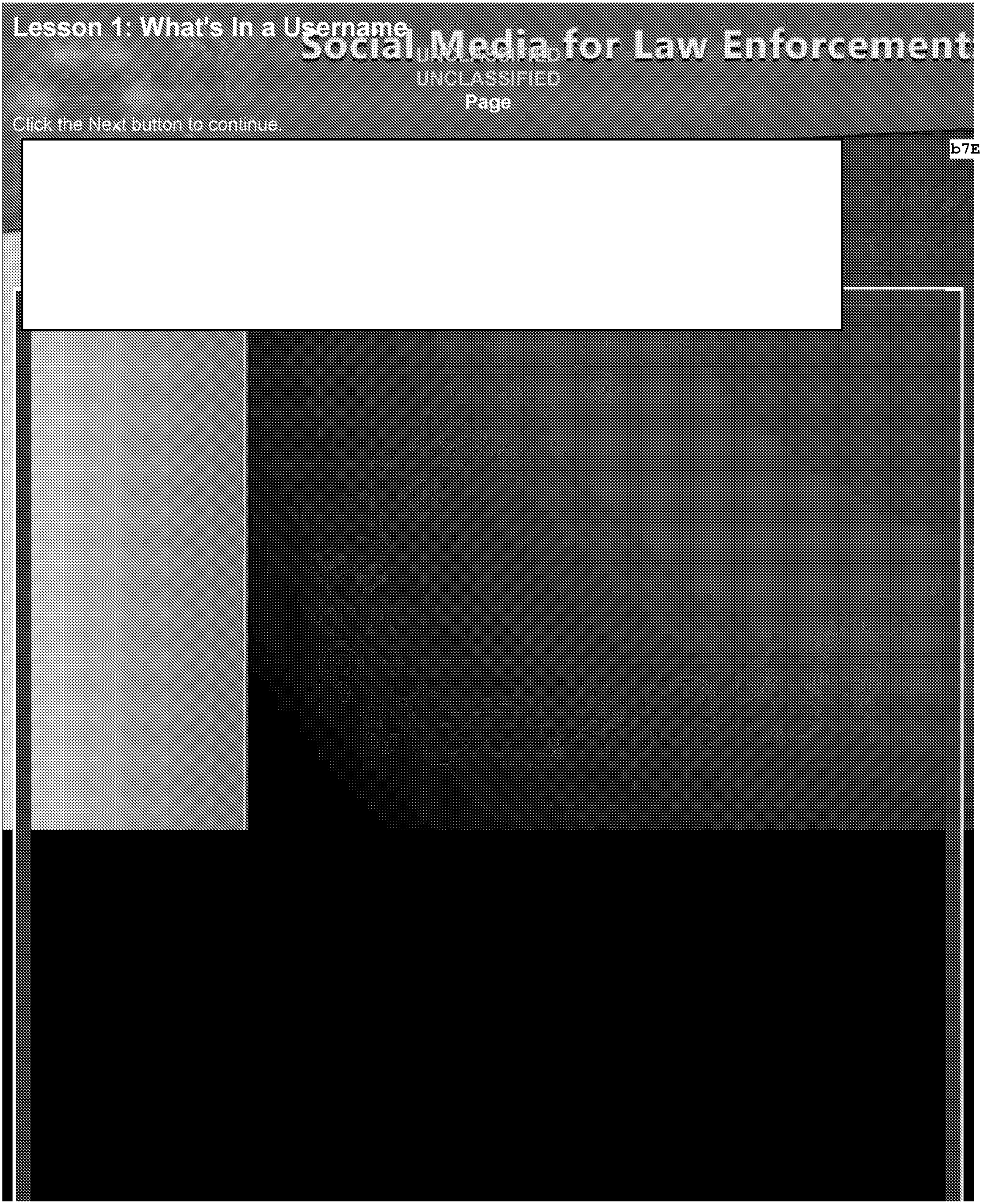
Select Lesson 2 from the sidebar to continue.
"Current Lesson."
Lesonn #
"Current Lesson."
Lesson #

Conclusion

You have completed reviewing "

Select the next button to review .

Lesson 1: What's In a Username



Lesson 1: What's In a Username

Social Media for Law Enforcement

UNCLASSIFIED

UNCLASSIFIED

Page

Click the Next button to continue.

[redacted]

b7E

Conclusion

"Current Lesson

Page

You have completed

This lesson introduced you to the case you will be investigating during the course. You learned about the information already gathered and to the investigative work already conducted.

You were introduced to [redacted] a tool that is more useful than Google or Bing when searching social media sites. b7E

Now that you have completed this lesson, you should be able to:

- Perform a search on [redacted]
- Explain the advantages of using [redacted] over Google or Bing
- Identify the benefits of using [redacted]

Select the complete button () to unlock the next lesson.

Lesson 1: What's In a Username

Social Media for Law Enforcement

UNCLASSIFIED

UNCLASSIFIED

Page

[redacted]

b7E

Click on the key words to learn more.

CLOSE

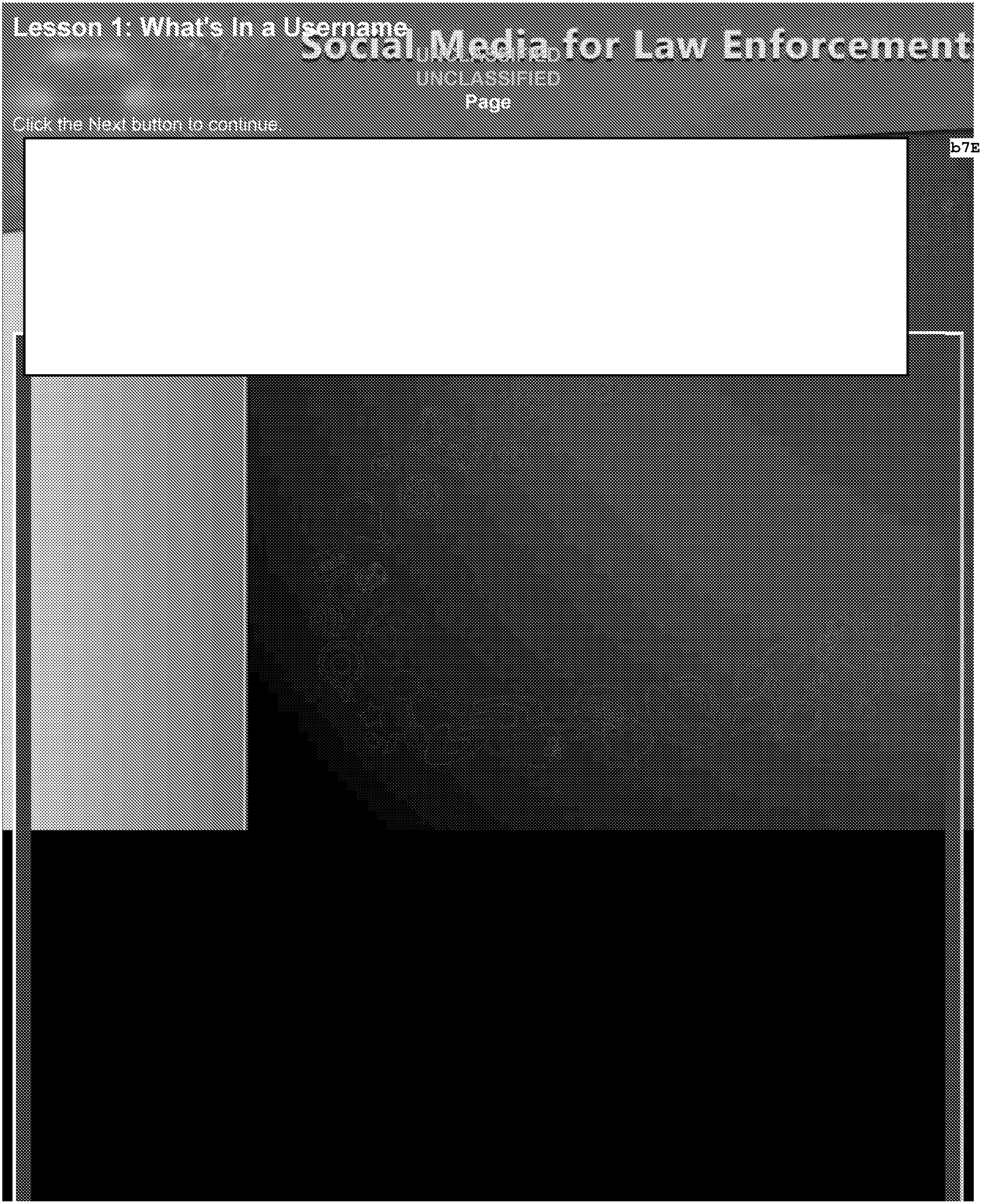
[redacted]

b7E

Deep Web refers to a vast repository of underlying content, such as documents in online databases that general-purpose web crawlers cannot reach. The deep web content is estimated at 500 times that of the surface web, yet has remained mostly untapped due to the limitations of traditional search engines. Any documents or information found through the deep web will still require investigators to contact the companies in possession of the information and present the required legal documents to acces the information. [redacted]

b7E

CLOSE



Lesson 1: What's In a Username

Social Media for Law Enforcement

UNCLASSIFIED

UNCLASSIFIED

Page

Click the Next button to continue.

[redacted]

b7E

Now is the time.

[redacted]

Lesson 2: Strategic Social Searches

Social Media for Law Enforcement

You have completed "

Select from the sidebar to continue.
"Current Lesson."
Lesson #
"Current Lesson."
Lesson #

UNCLASSIFIED

UNCLASSIFIED

Conclusion

You have completed reviewing "

Select the next button to review .

Introduction

Social Media for Law Enforcement

This lesson explores the steps that you would need to perform searches on [redacted] and to search [redacted] b7E [redacted]

After completing this lesson, you will be able to:

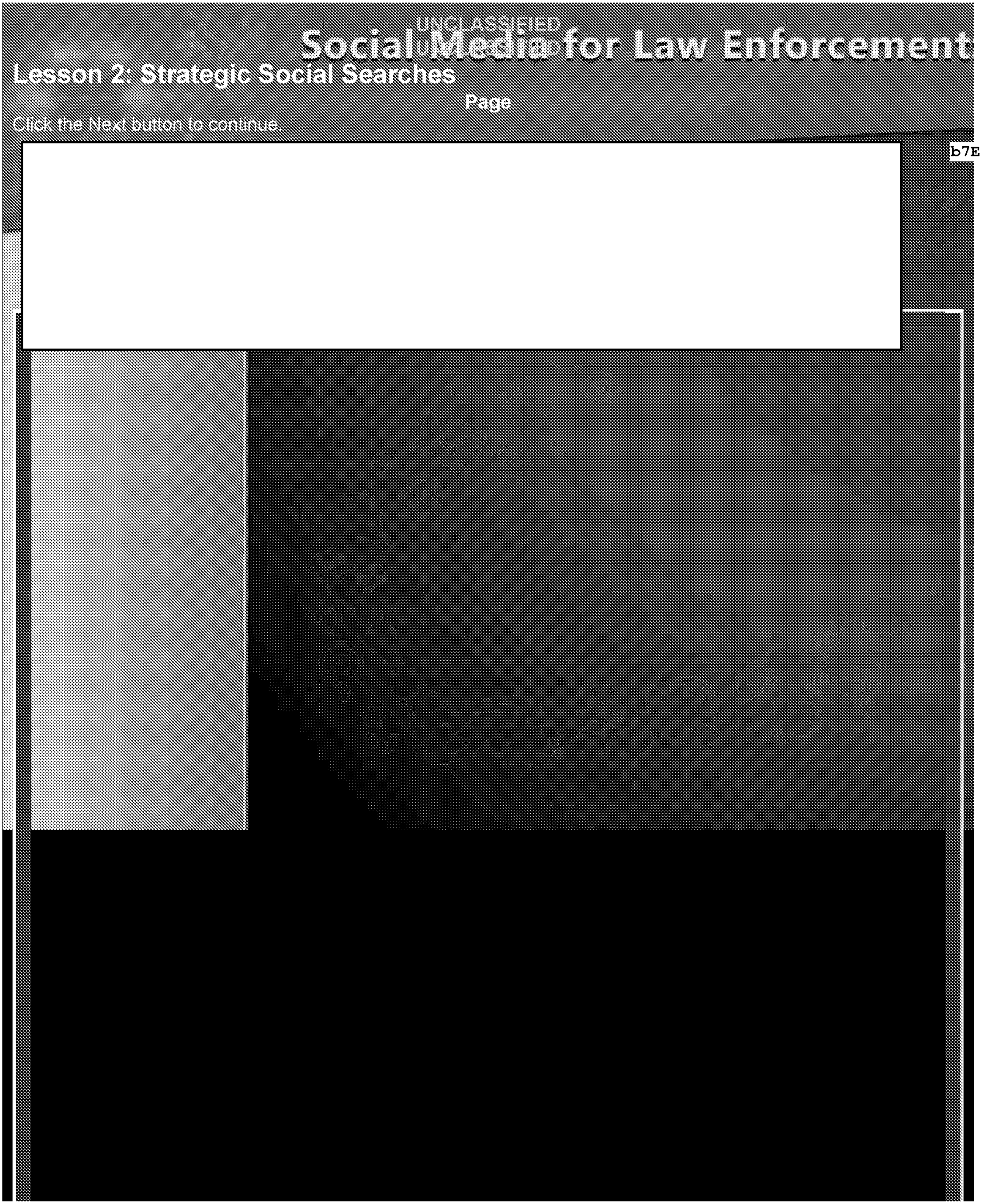
- Perform searches on [redacted]
- View and interpret results displayed on [redacted]
- Use a [redacted]
- Navigate through [redacted]

UNCLASSIFIED

UNCLASSIFIED

Lesson 2: Strategic Social Searches

Page



UNCLASSIFIED

Social Media for Law Enforcement

UNCLASSIFIED

Lesson 2: Strategic Social Searches

Page

Click the Next button to continue.

[redacted]

b7E

[redacted]

UNCLASSIFIED

Social Media for Law Enforcement

Lesson 2: Strategic Social Searches

Page

When it comes to social sites, despite an individual's efforts to keep their information private, [redacted]

b7E

[redacted]

UNCLASSIFIED

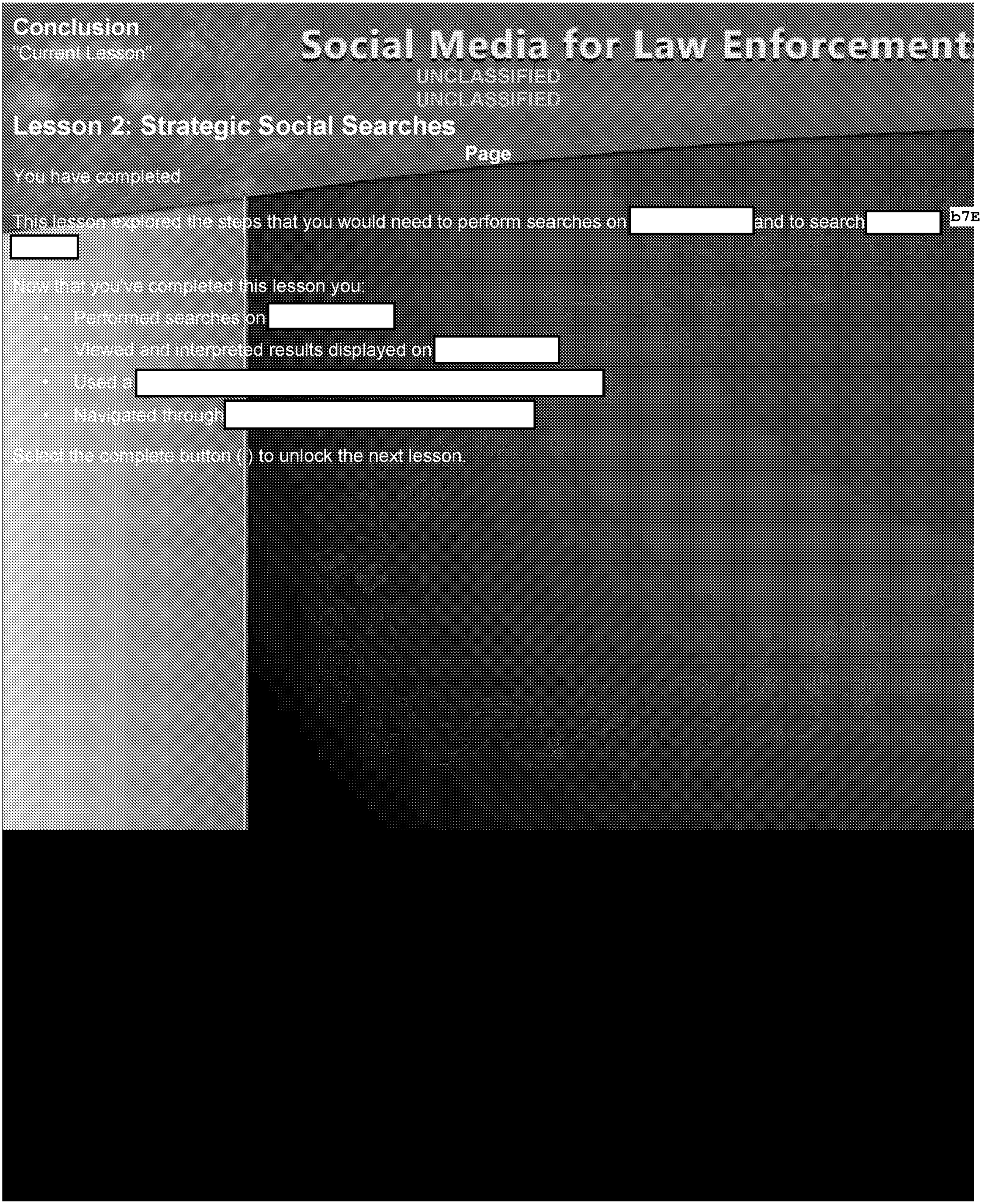
Social Media for Law Enforcement

UNCLASSIFIED

Lesson 2: Strategic Social Searches

Page

[redacted]



Conclusion

"Current Lesson"

Social Media for Law Enforcement

UNCLASSIFIED

UNCLASSIFIED

Lesson 2: Strategic Social Searches

Page

You have completed

This lesson explored the steps that you would need to perform searches on [redacted] and to search [redacted] b7E [redacted]

Now that you've completed this lesson you:

- Performed searches on [redacted]
- Viewed and interpreted results displayed on [redacted]
- Used a [redacted]
- Navigated through [redacted]

Select the complete button () to unlock the next lesson.

As with all search engines, [redacted] has an advanced search option that allows you to refine, or modify your search. b7E

Social Media for Law Enforcement

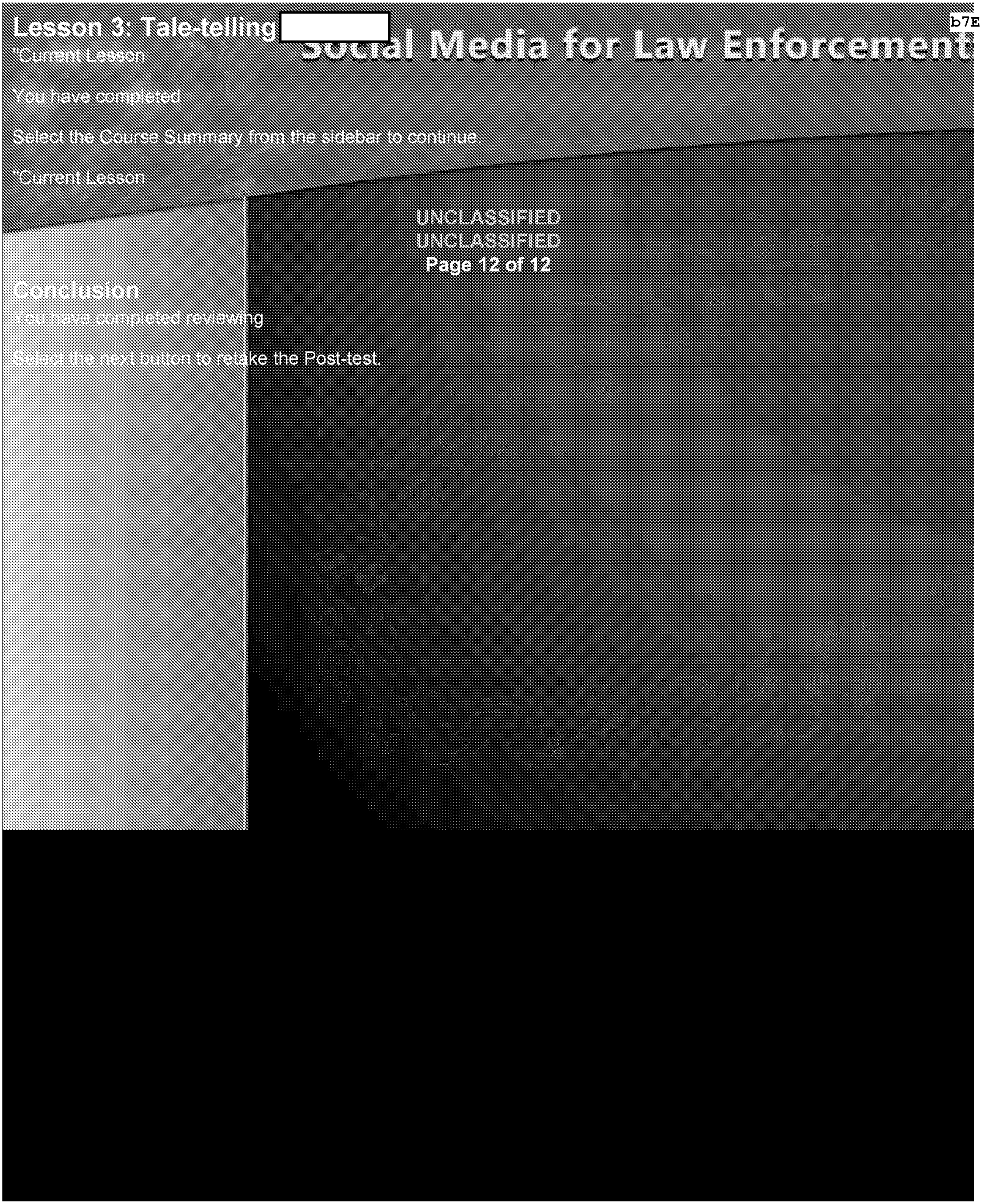
These advanced features can come in handy in an investigation.

UNCLASSIFIED

UNCLASSIFIED

Lesson 2: Strategic Social Searches

Page



Lesson 3: Tale-telling [redacted]

b7E

"Current Lesson

You have completed

Select the Course Summary from the sidebar to continue.

"Current Lesson

UNCLASSIFIED
UNCLASSIFIED
Page 12 of 12

Conclusion

You have completed reviewing

Select the next button to retake the Post-test.

Introduction

Social Media for Law Enforcement

This lesson introduces [redacted] which allows you to search for and view [redacted] b7E based on the given parameters. You will explore the steps needed to perform [redacted]

After completing this lesson, you will be able to:

- Perform [redacted] b7E
- Obtain [redacted] relevant to keywords
- Refine searches on [redacted]

UNCLASSIFIED

UNCLASSIFIED

Lesson 3: Tale-telling [redacted]

Page

Social Media for Law Enforcement

Lesson 3: Tale-telling [redacted]

b7E

Page

Social Media for Law Enforcemen

IMPORTANT NOTICE:

The U.S. Supreme Court ruled in a unanimous decision in Riley v. California that a search warrant is generally required to search the contents of a cell phone seized on an arrestee, and a warrantless search can no longer be conducted as part of a search incident to arrest exception to the 4th Amendment warrant requirement. Other exceptions to the warrant requirement continue to apply and arresting officers can also obtain the consent of an arrestee to search the contents of a phone without first obtaining a warrant.

Lesson 3: Tale-telling [redacted]

b7E

Page

Social Media for Law Enforcement

b7E

Lesson 3: Tale-telling [redacted] Page

Twitter's is a real-time information network that lets users share and discover what's happening now. Law enforcement must provide Twitter a subpoena for subscriber information.

Click to learn more:

Emergency Situations

Covert Investigation

Following a Feed

Joining an e-mail list or Twitter feed of an organization is participation that must abide by the policy of your organization. If the general public is not able to sign up to the twitter feed or the e-mail list, then additional approvals may be necessary.

CLOSE

It's important to note that most service providers have a policy to notify subscribers when law enforcement serves process for any information. In case of a covert investigation, you must submit a court order for non- disclosure along with a subpoena.

CLOSE

Emergency situations require an emergency disclosure request to obtain this information more quickly.

CLOSE

Lesson 3: Tale-telling [redacted] Page

b7E

Most Twitter profile information is public, so anyone can see it. A Twitter profile contains a profile photo, header photo, background image, and status updates, called tweets. In addition, the user has the option to fill out location, a URL, and a short "bio" section about themselves for display on their public profile.

[redacted]

UNCLASSIFIED

Social Media for Law Enforcement

Lesson 3: Tale-telling Tweets

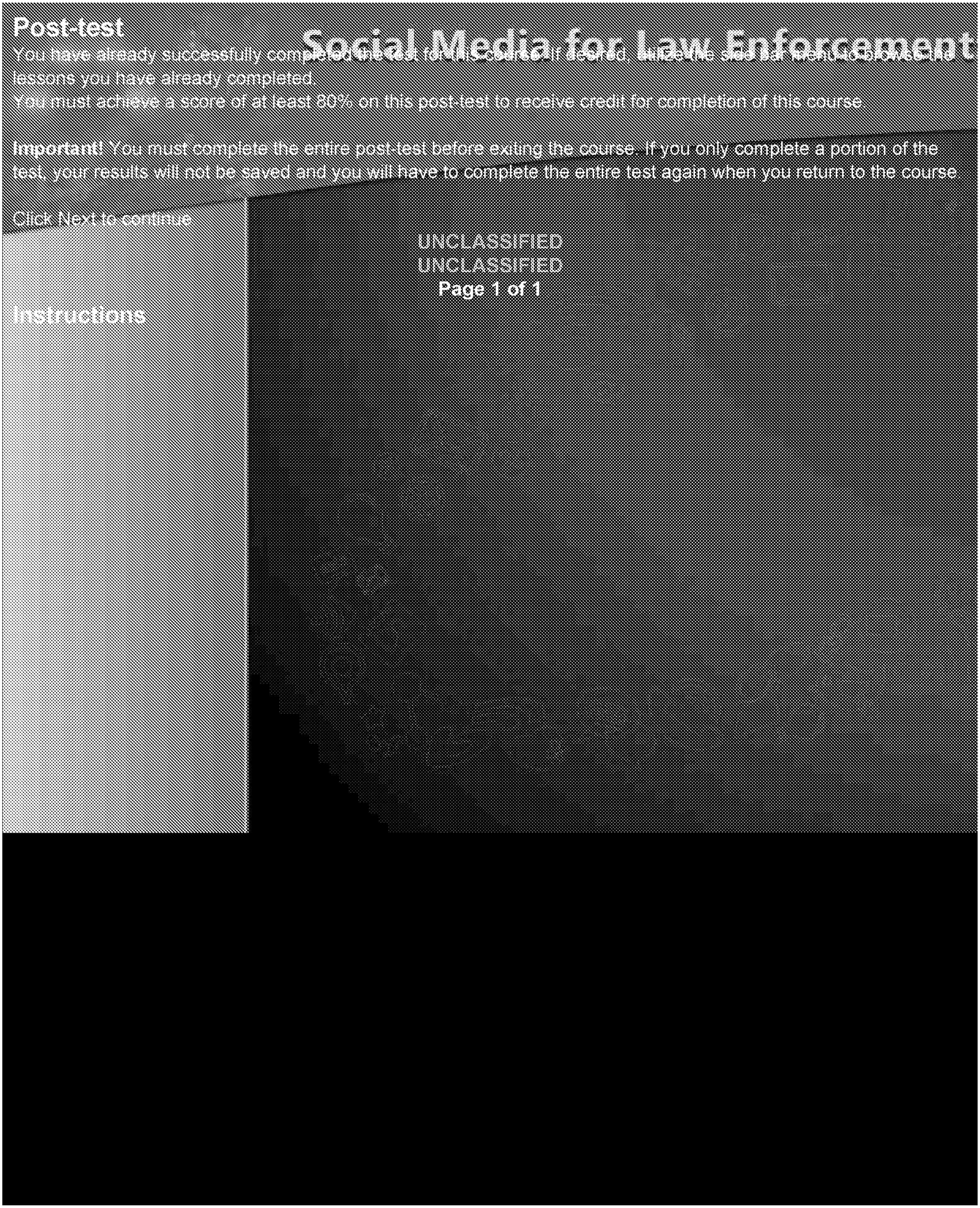
Page

Click the Next button to continue.

[redacted]

b7E

What Do You Think



Social Media for Law Enforcement

Post-test

You have already successfully completed the test for this course. If desired, utilize the side bar menu to browse the lessons you have already completed.

You must achieve a score of at least 80% on this post-test to receive credit for completion of this course.

Important! You must complete the entire post-test before exiting the course. If you only complete a portion of the test, your results will not be saved and you will have to complete the entire test again when you return to the course.

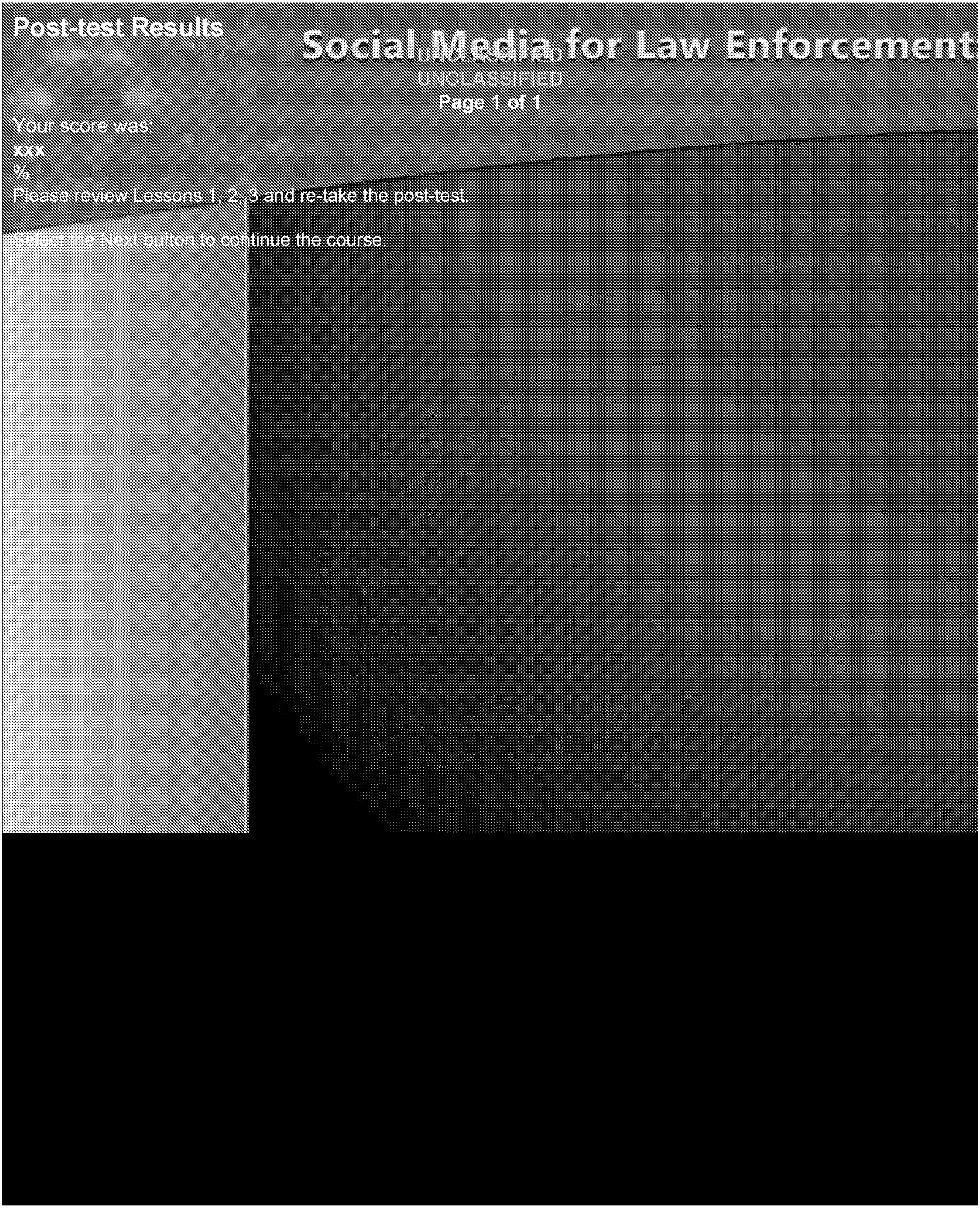
Click Next to continue

UNCLASSIFIED

UNCLASSIFIED

Page 1 of 1

Instructions



Post-test Results

Social Media for Law Enforcement

UNCLASSIFIED

UNCLASSIFIED

Page 1 of 1

Your score was:

xxx

%

Please review Lessons 1, 2, 3 and re-take the post-test.

Select the Next button to continue the course.

Post-test Results

Social Media for Law Enforcement

xxx

You have completed this course

Please complete the survey before exiting this course.

UNCLASSIFIED

UNCLASSIFIED

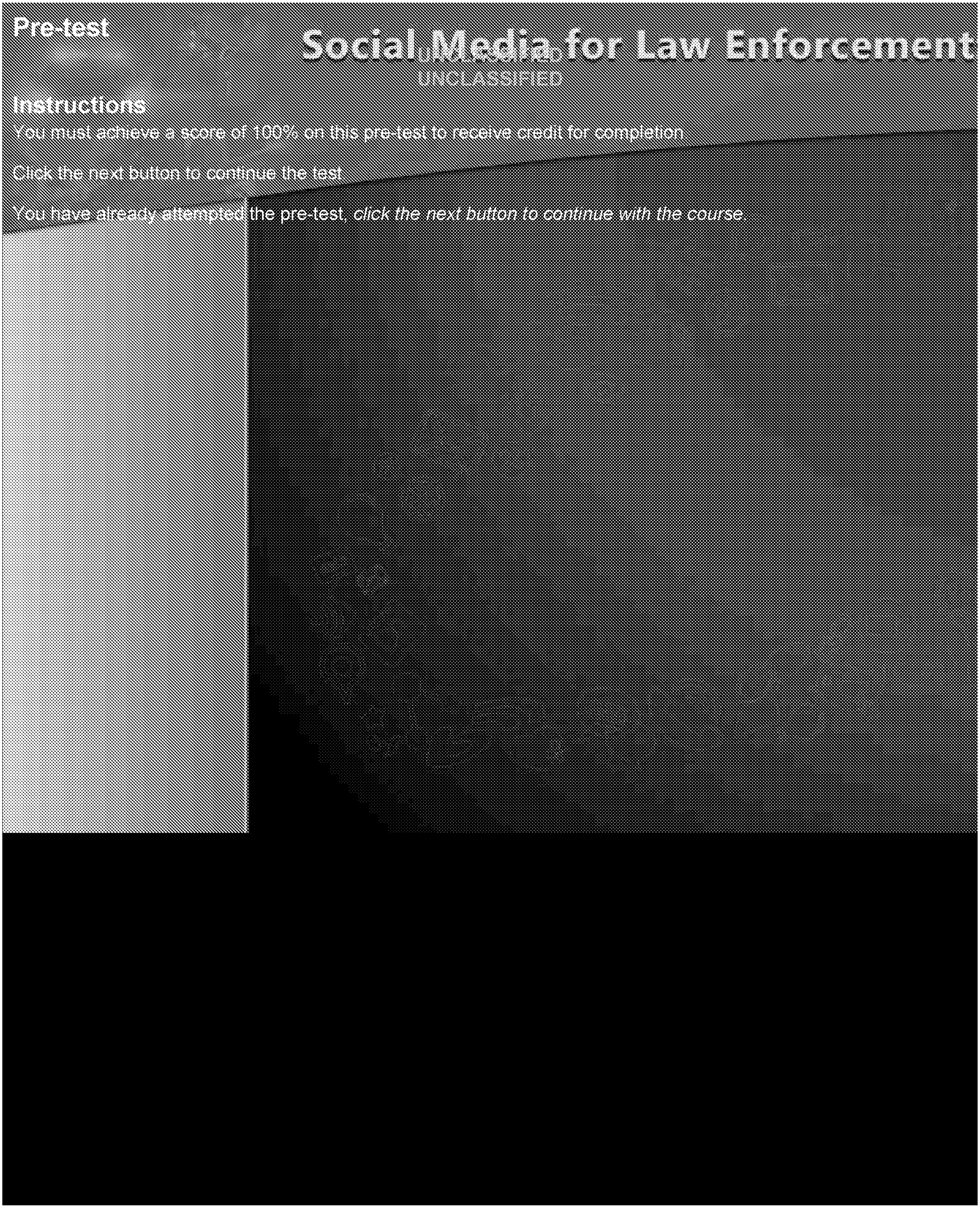
Page 1 of 1

Congratulations! You have passed the post-test for the *Social Media: Friend or Foe* course with a score of

Your transcript will show successful completion of this course.

Select the complete button () to mark the course completed. If you want to review the course, select a lesson from the sidebar.

%



Pre-test

Social Media for Law Enforcement

UNCLASSIFIED

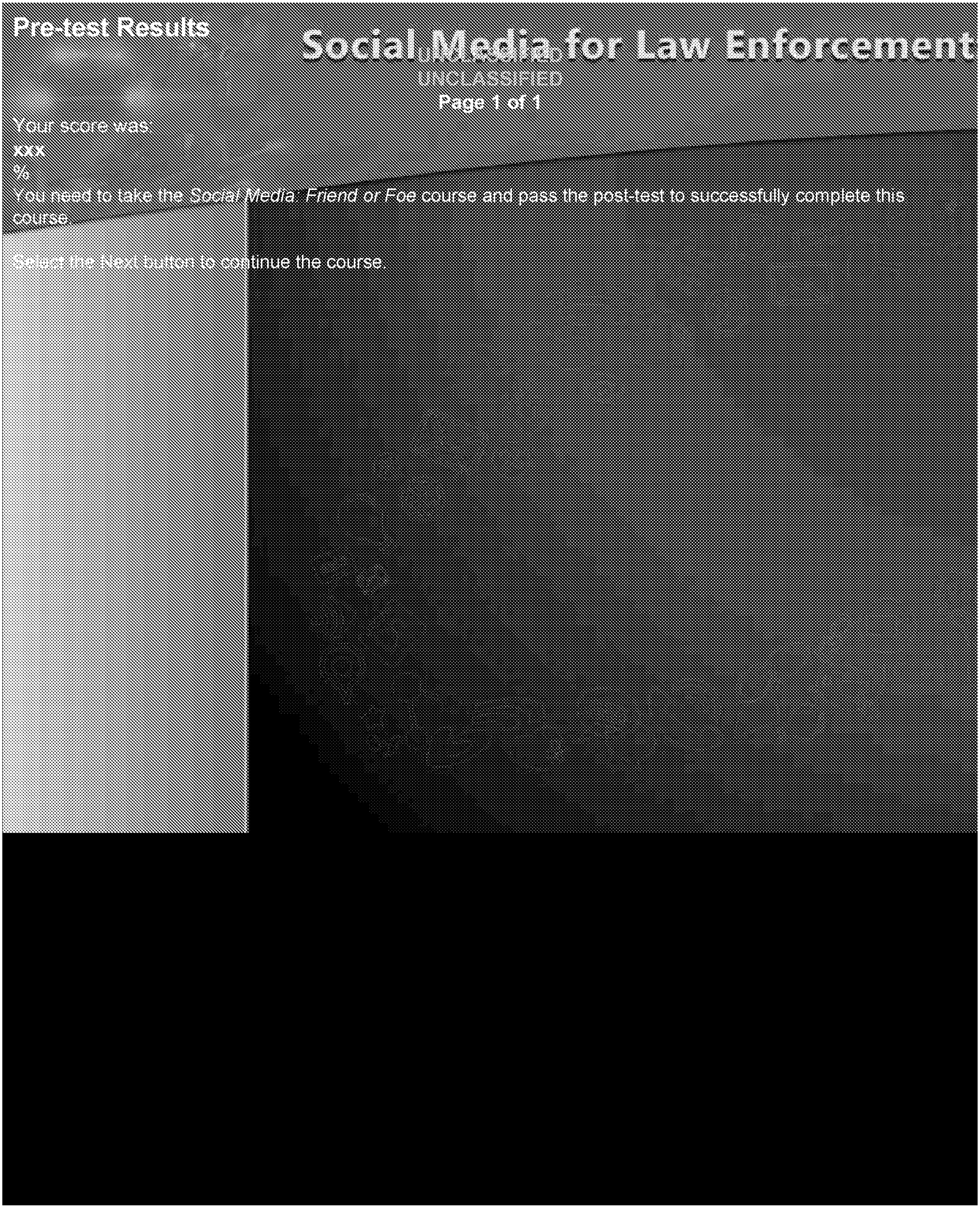
UNCLASSIFIED

Instructions

You must achieve a score of 100% on this pre-test to receive credit for completion.

Click the next button to continue the test.

You have already attempted the pre-test, *click the next button to continue with the course.*



Pre-test Results

Social Media for Law Enforcement

UNCLASSIFIED

UNCLASSIFIED

Page 1 of 1

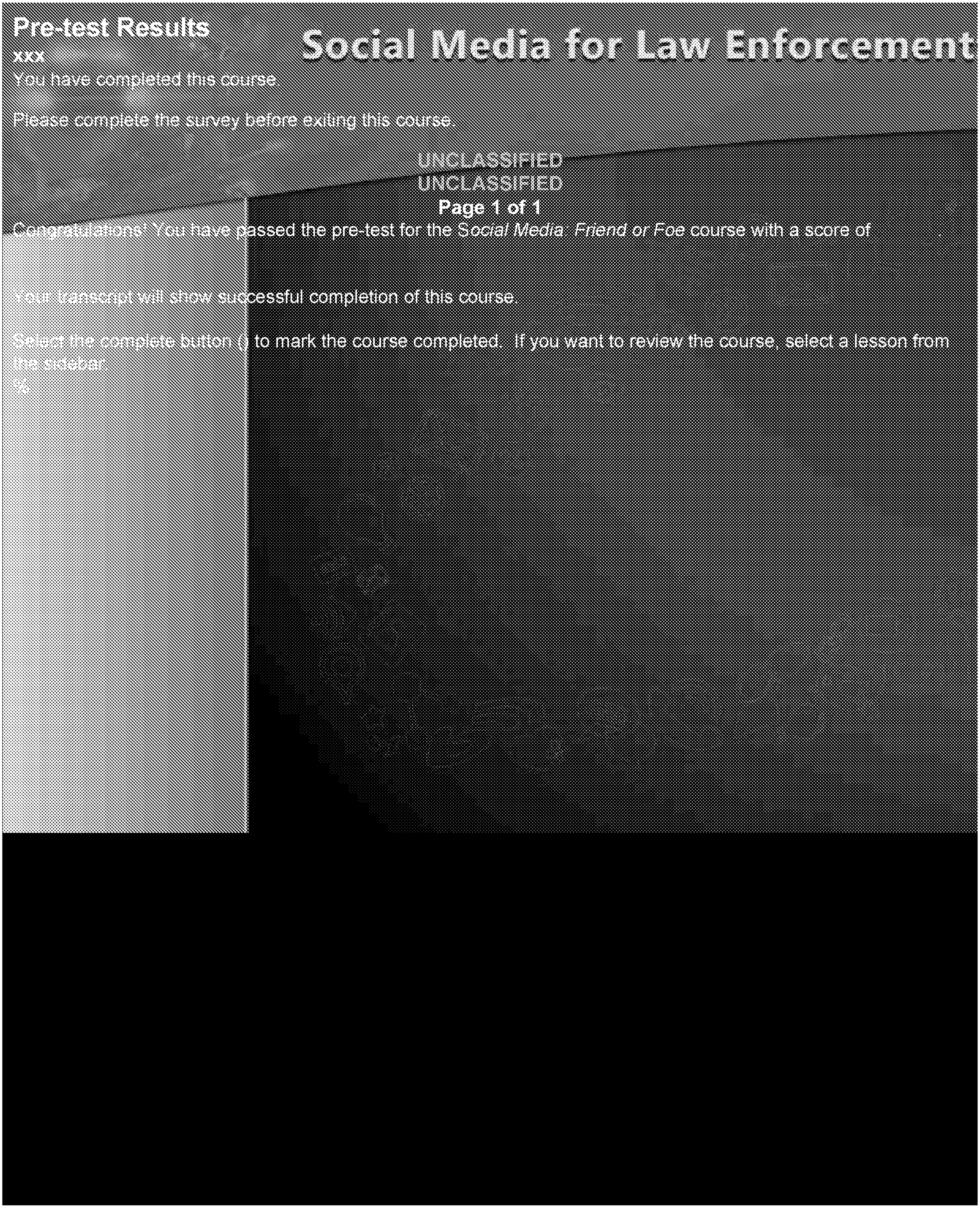
Your score was:

xxx

%

You need to take the *Social Media: Friend or Foe* course and pass the post-test to successfully complete this course.

Select the Next button to continue the course.



Social Media for Law Enforcement

Pre-test Results

xxx

You have completed this course

Please complete the survey before exiting this course.

UNCLASSIFIED

UNCLASSIFIED

Page 1 of 1

Congratulations! You have passed the pre-test for the *Social Media: Friend or Foe* course with a score of

Your transcript will show successful completion of this course.

Select the complete button () to mark the course completed. If you want to review the course, select a lesson from the sidebar.

%

Social Media for Law Enforcement

[redacted]

UNCLASSIFIED

Social Media for Law Enforcement

This course is sponsored by the Training Division.

UNCLASSIFIED

UNCLASSIFIED

Post-test

Social Media for Law Enforcement

Question

[redacted]

Post-Test

Exit

Glossary

Printer

Guidelines

Tools and Capabilities

Previous

Next

Question

Pre-test

Social Media for Law Enforcement

UNCLASSIFIED

UNCLASSIFIED

Question

[redacted]

Pre-Test

UNCLASSIFIED

Exit
Glossary
Previous
Next

Question

Glossary - Social Media: Friend or Foe

[redacted] b7E

Facebook®: An online social networking service; a platform to build social networks or social relations among people who, for example, share interests, activities, backgrounds, or real-life connections. This service consists of a representation of each user (often a profile), his/her social links, and a variety of additional services.

Internet Protocol Address (IP Address): A numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication. An IP address serves two principal functions: host or network interface identification and location addressing. Its role has been characterized as follows: "*A name indicates what we seek. An address indicates where it is. A route indicates how to get there.*" Internet Protocol – DARPA Internet Program Protocol Specification (September 1981).

Legat: The FBI has offices around the globe. These offices—called legal attachés or legats—are located in U.S. embassies.

Malware: Short for malicious (or malevolent) software, malware is software used or programmed by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. 'Malware' is a general term used to refer to a variety of forms of hostile or intrusive software.

Malware includes computer viruses, ransomware, worms, trojan horses, rootkits, keyloggers, dialers, spyware, adware, malicious BHOs, rogue security software and other malicious programs; the majority of active malware threats are usually worms or trojans rather than viruses. In law, malware is sometimes known as a computer contaminant, as in the legal codes of several U.S. states.

[redacted] b7E

Non-Attributable Computer: A computer that keeps others from linking its online activity to the FBI. A computer in which an investigator may perform online searches or investigations without permitting or disclosing any links to the FBI.

[redacted]

[redacted] b7E

Sensitive Investigative Matter (SIM): A sensitive investigative matter is defined as an investigative matter involving the activities of a domestic public official or political candidate (involving corruption or a threat to the national security), religious or political organization or individual prominent in such an organization, or news media, or any other matter which, in the judgment of the official authorizes an investigation, should be brought to the attention of FBI Headquarters and other DOJ officials. As a matter of FBI policy, "judgment" means that the decision of the authorizing official is discretionary.

Social Media: The means of interactions among people in which they create, share, and exchange information and ideas in virtual communities and networks. social media depend on mobile and web-based technologies to create highly interactive platforms through which individuals and communities share, co-create, discuss, and modify user-generated content. It introduces substantial and pervasive changes to communication between organizations, communities and individuals.

Social Network: A social structure made up of a set of social actors (such as individuals or organizations) and a complex set of the dyadic ties between these actors.

[redacted]

[redacted] b7E

Tweet: A text-based message found in Twitter of up to 140 characters.

Twitter®: An online social networking and micro-blogging service that enables its users to send and read text-based messages of up to 140 characters, known as "tweets."

Username: An identification used by a person with access to a computer network.

Vetted: A background check performed on intelligence gathered. Assets are vetted to determine their usefulness and reliability.

Social Media Guidelines for Law Enforcement

Facebook Pg 1, Twitter Pg 5, Instagram Pg 10, Pinterest Pg 14, Snapchat Pg 19, LinkedIn Pg 25.

FACEBOOK

Topics Covered

IMPORTANT

These operational guidelines are for law enforcement officials seeking records from Facebook. For private party requests, including requests from civil litigants and criminal defendants, visit: facebook.com/help/?page=1057. Users seeking information on their own accounts can access Facebook's "Download Your Information" feature from their account settings. See facebook.com/help/?page=18830. This information may change at any time.

US Legal Process Requirements

We disclose account records solely in accordance with our terms of service and applicable law, including the federal Stored Communications Act ("SCA"), 18 U.S.C. Sections 2701-2712 Under US law:

- A valid subpoena issued in connection with an official criminal investigation is required to compel the disclosure of basic subscriber records (defined in 18 U.S.C. Section 2703(c)(2)), which may include: name, length of service, credit card information, email address(es), and a recent login/logout IP address(es), if available.

- A court order issued under 18 U.S.C. Section 2703(d) is required to compel the disclosure of certain records or other information pertaining to the account, not including contents of communications, which may include message headers and IP addresses, in addition to the basic subscriber records identified above.

- A search warrant issued under the procedures described in the Federal Rules of Criminal Procedure or equivalent state warrant procedures upon a showing of probable cause is required to compel the disclosure of the stored contents of any account, which may include messages, photos, videos, wall posts, and location information.

- We interpret the national security letter provision as applied to Facebook to require the production of only 2 categories of information: name and length of service.

International Legal Process Requirements

We disclose account records solely in accordance with our terms of service and applicable law. A Mutual Legal Assistance Treaty request or letter rogatory may be required to compel the disclosure of the contents of an account. Further information can be found here: facebook.com/about/privacy/other.

Account Preservation

We will take steps to preserve account records in connection with official criminal investigations for 90 days pending our receipt of formal legal process. You may expeditiously submit formal preservation requests through the Law Enforcement Online Request System at facebook.com/records, or by email, fax or mail as indicated below.

Emergency Requests

In responding to a matter involving imminent harm to a child or risk of death or serious physical injury to any person and requiring disclosure of information without delay, a law enforcement official may submit a request through the Law Enforcement Online Request System at facebook.com/records. Important note: We will not review or respond to messages sent to this email address by non-law enforcement officials. Users aware of an emergency situation should immediately and directly contact local law enforcement officials.

Child Safety Matters

We report all apparent instances of child exploitation appearing on our site from anywhere in the world to the National Center for Missing and Exploited Children (NCMEC), including content drawn to our attention by government requests. NCMEC coordinates with the International Center for Missing and Exploited Children and law enforcement authorities from around the world. If a request relates to a child exploitation or safety matter, please specify those circumstances (and include relevant NCMEC report identifiers) in the request to ensure that we are able to address these matters expeditiously and effectively.

Data Retention and Availability

We will search for and disclose data that is specified with particularity in an appropriate form of legal process and which we are reasonably able to locate and retrieve. We do not retain data for law enforcement purposes unless we receive a valid preservation request before a user has deleted that content from our service. Details about data and account deletion can be found in our Data Use Policy (facebook.com/policy.php), Statement of Rights and Responsibilities (facebook.com/terms.php), and Help Center (facebook.com/help/?faq=224562897555674).

Form of Requests

We will be unable to process overly broad or vague requests. All requests must identify requested records with particularity and include the following:

- The name of the issuing authority, badge/ID number of responsible agent, email address from a law-enforcement domain, and direct contact phone number.

- The email address, user ID number (http://www.facebook.com/profile.php?id=1000000XXXXXXXX) or username (http://www.facebook.com/username) of the Facebook profile.

User Consent

If a law enforcement official is seeking information about a Facebook user who has provided consent for the official to access or obtain the user's account information, the user should be directed to obtain that information on their own from their account. For account content, such as messages, photos, videos and wall posts, users can access Facebook's "Download Your Information" feature from their account settings. See facebook.com/help/?page=18830. Users can also view recent IP addresses in their Account Settings under Security Settings/Active Sessions. Users do not have access to historical IP information without legal process.

Notification

Law enforcement officials who believe that notification would jeopardize an investigation should obtain an appropriate court order or other process establishing that notice is prohibited. Law enforcement officials may also request nondisclosure if notice would lead to risk of harm. If your data request draws attention to an ongoing violation of our terms of use, we will take action to prevent further abuse, including actions that may notify the user that we are aware of their misconduct.

Testimony

Facebook does not provide expert testimony support. In addition, Facebook records are self-authenticating pursuant to law and should not require the testimony of a records custodian. If a special form of certification is required, please attach it to your records request.

Cost Reimbursement

We may seek reimbursement for costs in responding to requests for information as provided by law. These fees apply on a per account basis. We may also charge additional fees for costs incurred in responding to unusual or burdensome requests. We may waive these fees in matters investigating potential harm to children, Facebook and our users, and emergency requests.

Submission of Requests Online

Law enforcement officials may use the Law Enforcement Online Request System at facebook.com/records for the submission, tracking and processing of requests. Please note that a government-issued email address is required to access the Law Enforcement Online Request System. You may also submit requests by email or fax as indicated below.

Email

records@facebook.com

Fax

United States: +1 650 472-8007
Ireland: +353 (0)1 653 5373

Mail

United States Mail Address: 1601 Willow Road, Menlo Park CA 94025 Ireland Mail Address: Hanover Reach | 5-7 Hanover Quay, | Dublin 2 Attention: Facebook Security, Law Enforcement Response Team Law enforcement officials who do not submit requests through the Law Enforcement Online Request System at facebook.com/records should expect longer response times.

Notes

- Acceptance of legal process by any of these means is for convenience and does not waive any objections, including lack of jurisdiction or proper service.

- We will not respond to correspondence sent by non-law enforcement officials to the addresses above.

TWITTER

Topics Covered

IMPORTANT

These guidelines are intended for law enforcement personnel seeking to request information about Twitter users. Information regarding requests to withhold content is available on our Country Withheld Content article (https://support.twitter.com/articles/20169222); requests can be filed through our web form. More general information on Twitter's Rules can be found here (https://support.twitter.com/articles/18311).

What is Twitter?

Twitter is a real-time information network powered by people all around the world that lets users share and discover what's happening now. Users send 140-character messages through our website and mobile site, client applications, or any variety of third-party applications. For more information, you can also visit https://twitter.com/about (https://twitter.com/about). For the latest on Twitter's features and functions please visit our Help Center (https://support.twitter.com).

What User Information Does Twitter Have?

User information is held by Twitter, Inc. in accordance with our Privacy Policy (https://twitter.com/privacy) and Terms of Service (https://twitter.com/tos). We require a subpoena, court order, or other valid legal process to disclose information about our users. Most Twitter profile information is public, so anyone can see it. A Twitter profile contains a profile photo, header photo, background image, and status updates, called Tweets. In addition, the user has the option to fill out location, a URL, and a short "bio" section about themselves for display on their public profile. Please see our Privacy Policy (https://twitter.com/privacy) for more information on the data we collect from users.

Does Twitter Have Access to User Photos or Videos?

Twitter provides photo hosting for some image uploads (i.e., pic.twitter.com) as well as a user's profile photo, header photo, and account background image; Twitter does not, however, provide hosting for videos other than those posted to Vine (https://support.twitter.com/articles/20170317), nor is Twitter the sole photo hosting provider for images that may appear on the Twitter service. More information about posting photos on Twitter can be found here (https://support.twitter.com/articles/20156423).

Data Retention Information

Twitter retains different types of information for different time periods. Given Twitter's real-time nature, some information may only be stored for a very brief period of time. Information on our retention policies can be found in our Privacy Policy.

Preservation Requests

We accept requests from law enforcement to preserve records pending the issuance of valid legal process. Preservation requests, in accordance with applicable law, should be signed by the requesting official, include the @username and URL of the subject Twitter profile (e.g., @safety and https://twitter.com/safety (https://twitter.com/safety)), have a valid return email address, and be sent on law enforcement letterhead. Requests may be sent via the methods described below.

Requests for User Information

Twitter, Inc. is located in San Francisco, California and will only respond to valid legal process in compliance with U.S. law.

Private Information Requirements: Subpoena vs. Court Order

In accordance with our Privacy Policy (https://twitter.com/privacy) and Terms of Service (https://twitter.com/tos), non-public information about Twitter users is not released except as lawfully required by appropriate legal process such as a subpoena, court order, or other valid legal process. Some information we store is automatically collected, while other information is provided at the user's discretion. Though we do store this information, it may not be accurate if the user has created a fake or anonymous profile. Twitter doesn't require email verification or identity authentication. **Contents of Communications Requires a Search Warrant.** Requests for the contents of communications (e.g., Tweets, DMs, photos) require a valid U.S. search warrant.

Will Twitter Notify Users of Requests for Account Information?

Yes. Twitter's policy is to notify users of requests for their information prior to disclosure unless we are prohibited from doing so by statute or court order (e.g., an order under 18 U.S.C. § 2705(b) (http://www.law.cornell.edu/uscode/text/18/2705)).

What Information Must Be Included?

When requesting user information, please include:
The @username and URL of the subject Twitter profile in question (e.g., @safety and https://twitter.com/safety (https://twitter.com/safety)); Details about what specific information is requested (e.g., basic subscriber information) and its relationship to your investigation;

Note: Please ensure that the information you seek is not available from our public API. We are unable to process overly broad or vague requests. A VALID EMAIL ADDRESS so we may get back in touch with you upon receipt of your legal process. Requests may be submitted by fax or mail; our contact information is available at the bottom of these Guidelines.

NOTE: We do not accept legal process via email at this time; our support system automatically removes all attachments for security reasons.

Production of Records

Unless otherwise agreed upon, we currently provide responsive records in electronic format (i.e., plain text files that can be opened with any word processing software such as Word or TextEdit).

Records Authentication

The records that we produce are self-authenticating. Additionally, the records are electronically signed to ensure their integrity at the time of production. If you require a declaration, please note that in your request.

Emergency Disclosure Requests

Twitter evaluates emergency disclosure requests on a case-by-case basis in compliance with 18 U.S.C. §

2702(b)(8) (http://www.law.cornell.edu/uscode/text/18/2702). If we receive information that gives us a good faith belief that there is an exigent emergency involving the danger of death or serious physical injury to a person, we may provide information necessary to prevent that harm, if we have it.

How to Make an Emergency Disclosure Request

If there is an exigent emergency that involves the danger of death or serious physical injury to a person that Twitter may have information necessary to prevent, you can submit an emergency disclosure request through our web form (https://support.twitter.com/forms/lawenforcement) (the quickest and most efficient method). Alternatively, you may fax emergency requests to 1-415-222-9958 (faxed requests may result in a delayed response); please include all of the following information:

- Please indicate on your cover sheet that you're submitting an Emergency Disclosure Request
- Identify the person who is in danger of death or serious physical injury
- The nature of the emergency (e.g., report of suicide, bomb threat)
- Twitter @username and URL (e.g., @safety and https://twitter.com/safety (https://twitter.com/safety)) of the subject account(s) whose information is necessary to prevent the emergency
- Any specific Tweets (https://support.twitter.com/articles/80586) you would like us to review
- The specific information requested and why that information is necessary to prevent the emergency
- All other available details or context regarding the particular circumstances

Requests from Non-U.S. Law Enforcement

U.S. law authorizes Twitter to respond to requests for user information from foreign law enforcement agencies that are issued via U.S. court either by way of a mutual legal assistance treaty (“MLAT”) or a letter rogatory. It is our policy to respond to such U.S. court ordered requests when properly served. Non-U.S. law enforcement authorities may also submit requests for emergency disclosure under exigent circumstances, as outlined in the section titled "How to Make an Emergency Disclosure Request," above.

Assisting a Twitter User

If you are assisting a Twitter user with an investigation and want to obtain a copy of the Twitter user’s nonpublic account information, please instruct the user to contact us directly (see below) to request his or her own information.

- **Tweets Archive** – Twitter provides each registered user with the capacity to obtain a download of Tweets posted to their personal account. More information on how a user can request that information is available in our Help Center:
    - https://support.twitter.com/articles/20170160 (https://support.twitter.com/articles/20170160).

- **Non-Public Information** – Twitter does not currently offer users a self-serve method to obtain other, non-public information (e.g., IP logs) about their accounts. If a Twitter user has provided consent to law enforcement to obtain his or her nonpublic account information, please direct the user to request this information directly from Twitter by sending an email to privacy@twitter.com (mailto:privacy@twitter.com) with subject: Request for Own Account Information; we will respond with further instructions.

- **Other Issues** – Most issues can be resolved by having users to submit inquires directly to us. More information on how to report violations is available here: https://support.twitter.com/articles/15789 (https://support.twitter.com/articles/15789).

General Inquiries

Other general inquiries from law enforcement / government officials can be submitted through our web form (https://support.twitter.com/forms/lawenforcement).

Contact Information

You may fax Twitter, Inc., c/o Trust & Safety – Legal Policy, at: 1-415-222-9958.

Our mailing address is:
Twitter, Inc.
c/o Trust & Safety - Legal Policy
1355 Market Street Suite 900
San Francisco, CA 94103

Receipt of correspondence by any of these means is for convenience only and does not waive any objections, including the lack of jurisdiction or proper service. Non-law enforcement requests should be sent through our regular support methods (https://support.twitter.com (https://support.twitter.com/)).

Tweet

INSTAGRAM

Topics Covered

What is Instagram?

Instagram is a fast, beautiful and fun way to share your life with friends through a series of pictures. These pictures are shared on Instagram, and can be easily uploaded to other social media platforms including Twitter, Facebook, and Tumblr.

You can find more information in our Press Center and Support Center.

Requests for User Information

We disclose account records solely in accordance with our terms of service and applicable law, including the federal Stored Communications Act ("SCA"), 18 U.S.C. Sections 2701-2712. Under the SCA:

- A valid subpoena issued in connection with an official criminal investigation is required to compel the disclosure of basic subscriber records (defined in 18 U.S.C. Section 2703(c)(2)), which may include: subscriber name, phone number, account creation date, email address, and a signup IP address, if available.

- A court order issued under 18 U.S.C. Section 2703(d) is required to compel the disclosure of certain records or other information pertaining to the account, not including contents of communications, which may include photographs, photo captions, and other electronic communication information in addition to the basic subscriber records identified above.

- A search warrant issued under the procedures described in the Federal Rules of Criminal Procedure or equivalent State warrant procedures upon a showing of probable cause is required to compel the disclosure of the stored contents of any account, which may include messages, photos, comments, and location information.

It is important to note that some information we store is collected automatically, while other information is provided by the user, and that we do not require email or identity verification. If a user has created a fake or anonymous profile, our information may not be authentic. We are unable to process overly broad or vague requests.

For reference, please read our Privacy Policy and Terms of Use.

Data Retention and Availability

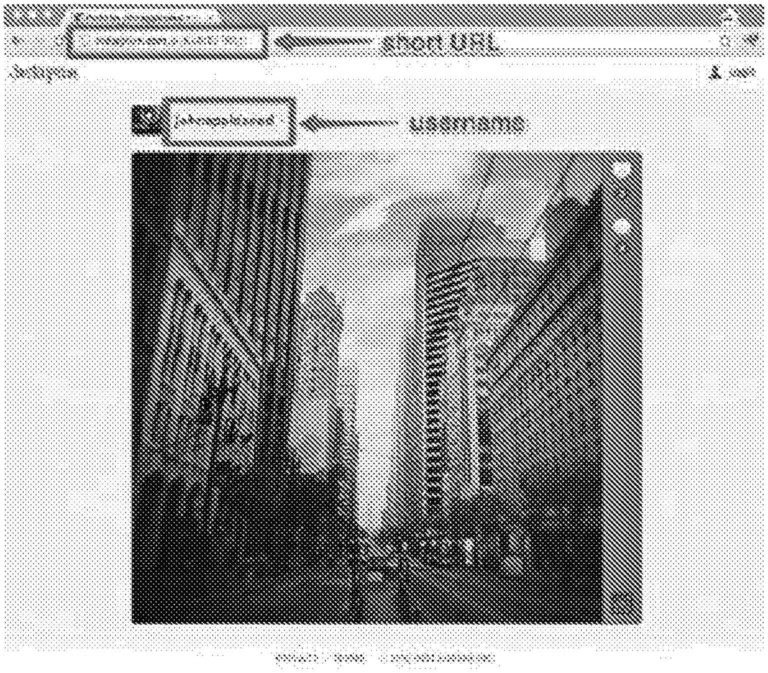
We retain different types of information for different time periods. Given the volume of real-time content on Instagram, some information may only be stored for a short period of time. We do not retain data for law enforcement purposes unless we receive a valid preservation request. Preservation requests must include the username of the Instagram account in question, a valid return email address, and must be signed and sent on law enforcement letterhead.

Information to Include

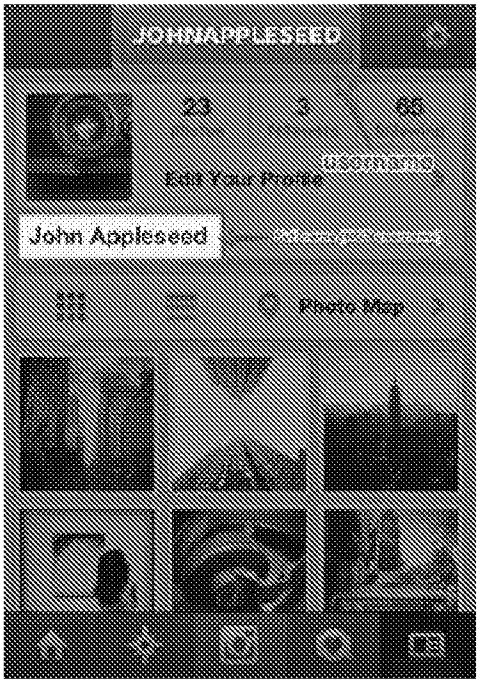
All requests must identify the following:

1. The name of the issuing authority, badge/ID number of responsible agent, email address from a law enforcement domain, and a direct contact phone number.
2. The username of the Instagram account in question and details regarding specific information requested and its relationship to your investigation.

3. If you have access to an image's short URL, you can locate the username here:



4. If you have access to the Instagram application, you can locate the username here:



Emergency Requests

Matters involving anticipated harm to a child or risk of death or serious physical injury to any person that requires disclosure of information without delay should contact us at lawenforcement@instagram.com.

It is important to note that we will not review or respond to messages sent to this email address by non-law enforcement officials. If you are a user aware of an emergency situation, you should immediately and directly contact local law enforcement officials.

Contact Information

Law enforcement officers may submit all records requests by email or mail.

Only email from law enforcement domains will be accepted. All others will be disregarded. Non-law enforcement requests should be sent through our regular support methods via Instagram's Support Center.

Email: lawenforcement@instagram.com

Mail:
Attn: Instagram Law Enforcement Response Team
1601 Willow Road
Menlo Park, CA 94025

PINTEREST

Topics Covered

IMPORTANT

Every company that stores information -- from banks to phone companies to email providers -- should have policies and guidelines for responding to law enforcement requests for information. These are ours. This information is intended for law enforcement only. If you are not a member of law enforcement and have questions, visit our Help Center.

What's Pinterest?

Pinterest is an online tool for collecting, organizing and discovering interests. The people who use Pinterest are “pinners.” A pinner can "pin" a link to media content (ex: images, video or audio) from across the internet, or upload their own images to Pinterest (pinners can't upload audio or video directly to Pinterest right now).

Pinners collect their pins on boards. Pinners can invite other people to pin to a board with them.

Pinners can follow other people's boards, and pin, like or comment on other people's pins.

Pinners see the pins of the people or boards they follow in a chronologically ordered Home Feed.

Pinners can discover new pins, boards, and people by browsing our category feeds (ex: Popular, Design, Home Decor, Men's Fashion, etc.) or searching for specific content.

Pins

A pin is comprised of media content (an image, audio or video), a short description and a link. There are a few ways to pin, via: (1) pinterest.com, (2) the Pin It button for browsers, (3) the Pinterest mobile application (e.g. iOS or Android) and (4) a “pin it” button that third party content owners choose to embed on their websites.

When pinning, the pinner can customize the pin's description and choose the board to pin to.

Note: In some cases, the website/content owner prepopulates the pin's description with information about the content (ex: lazy_cat.jpg or “Confessional Cheesecake Recipe | via mbarton.org”). The pinner can always change this description while pinning.

The pinner may choose to write their own or edit the source and description after they have initially pinned the image or video. After pinning, the pinner can edit the description or source link. Pinners can also move pins between boards or pin the same pin to multiple boards.

Editing a Pin.

The pinner can can move pins between boards or repin the same item to multiple boards. More general information about pins.

Repins

A pinner can repin another pinner's pin, adding it to their own board. In some cases, the repin chain may be several repins away from the original pinner (X repinned it from Y who repinned it from Z, the original content poster).

If a pinner deletes a pin, it does not delete any of the repins of that pin from other people's boards.

Note: When repinning, the description is prepopulated with the description of the last pinner. The pinner can change this while repinning or edit the description any time after pinning.

Likes

Pinners can also like the pins of other pinners and they'll show up in the "Like" section of their profile. A pinner can unlike pins they have liked at anytime. Once unliked, the pin will no longer show up in their profile. All likes are public. Learn more about likes.

Comments

Any pinner can comment on pins they can see (for example, public or secret board that they contribute to). A pinner can delete comments they have made as well as comments other uses have made to pins they have created. Comments on pins are public, if the board is public. Learn more about comments.

Note: What looks like the first comment in a pin is actually the pin description - not a comment.

Profile

A pinner's profile is public and includes certain pinner-provided information (ex: name, profile picture) and a public summary of their boards, pins, likes, their followers and the people they're following. The pieces of information available on a profile are:

1) Name (required)
2) Username (required)
3) Location (not required)
4) Profile description with a 500 character limit (not required)
5) Website (not required)
6) Profile picture (not required)
7) Facebook or Twitter, if the pinner chooses to link to these accounts (not required)

Pinterest does not require that pinners provide their real name, nor do we verify the name or location they provide.

An unsuspended pinner may edit their profile information at anytime.

Board and Secret Boards

A board is a collection of pins usually organized around a pinner-defined interest or theme. Pinners can invite other people to add pins to their boards.

When creating a board, the pinner can make it public to everyone or secret. Once a board is public, it can't be made secret, but a pinner can convert a secret board to a public one. Learn more about boards and secret boards.

What pinner information does Pinterest have?

Pinterest stores and maintains pinner information as described in our Privacy Policy and the applicable Terms of Service [consumer, business]. You can find examples of information we store in our Privacy Policy.

We can't guarantee that the information described in the Privacy Policy or applicable Terms of Service will be available for any given pinner. Pinterest does not necessarily maintain a copy of the image, audio or video file a pinner pins. For example, pinners can link to video services like YouTube and the video is played through YouTube's API.

What does Pinterest require to produce pinner information?

For U.S. Law Enforcement

We will not provide any pinner's information unless you obtain a valid subpoena, court order or search warrant ("Law Enforcement Request"). We will not provide any pinner's content unless you obtain a valid search warrant.

For Non-U.S. Law Enforcement

We will not provide any pinner information unless you obtain a valid U.S. court order (via the mutual legal assistance treaties or letter rogatory).

What does Pinterest need to share pinner information with law enforcement?

To respond to your Law Enforcement Request(s), we'll need:

1. The applicable Law Enforcement Request we described above
2. The pinners username (pinterest.com/[username]) and/or email address used to create their Pinterest account
3. A valid return email address from an official government domain

In order to make sure your Law Enforcement Request is narrow and does not seek more information that necessary (potentially at additional cost and time), we ask for the following:

1. A sufficiently narrow/defined time period;
2. A specific event or action that the subject took;
3. A specific reference (ex:, Pin URL = http://pinterest.com/pin/424605071088241488/).

How do I request the preservation of and/or production of pinner information?

Pinterest must be notified in accordance with applicable U.S. law or valid legal process to this email address: lawenforcement@pinterest.com (We will only respond to emails from law enforcement. If you are not law enforcement and have an issue, please visit our Help Center). Electronic process only please.
Acceptance of legal process does not waive any objections Pinterest may have, including jurisdiction or proper service.

Do you notify pinners of a preservation request?

No, we only notify pinners of Law Enforcement Requests for their information.

Do you notify pinners of a Law Enforcement Request?

Yes, we notify pinners by providing them with a complete copy of the Law Enforcement Request before producing their information to law enforcement, unless prohibited by court order issued in accordance with 18 U.S.C. § 2705(b) or applicable statute.

Note: Officer authored affidavits, descriptions, cover letters or similar statements are not sufficient to preclude notice to our users. You must provide a court order issued in accordance with 18 U.S.C. § 2705(b) or cite an applicable statute if you wish to prohibit user notice of your Law Enforcement Request. Please contact us if you have any questions regarding this.

Do you include a copy of the Law Enforcement Request in your notice to pinners?

Yes, we include the complete Law Enforcement Request that was served on Pinterest when we notify the pinner (unless prohibited from notifying the user - see above).

What are the costs of preservation and/or production requests?

If we may seek reimbursement for the actual costs of preserving and/or producing information, Pinterest will provide a good faith estimate of such costs as part of our production or upon law enforcements request prior to our processing. Costs are based on the amount of data, time and resources required to process and query the raw data Pinterest maintains.

Do you provide a Certificate of Authentication or Expert Testimony?

Pinterest provides a certification from its records custodian with each production but is not generally able to provide in person testimony or expert witness.

Emergency Contact

If you are a pinner and aware of imminent harm to an individual or individuals, please contact local law enforcement authorities immediately.

In a situation where there is an emergency involving danger of death or serious physical injury, law enforcement can submit a request for disclosure of pinner information to Pinterest by contacting us:

> *Emergency Law Enforcement email: lawenforcement-emergency@pinterest.com (We will only respond to emails from law enforcement. If you are not law enforcement and have an issue, please visit our Help Center. Emailing this alias is considered abuse).*

Pinterest will review and respond to these requests on a case-by-case basis.

Miscellaneous

Do you maintain a transparency report?

Pinterest does not produce a transparency report at this time but we plan to in the near future.

I have questions about CyberTips, what should I do?

Please contact lawenforcement@pinterest.com (We will only respond to emails from law enforcement. If you are not law enforcement and have an issue, please visit our Help Center).

SNAPCHAT

Topics Covered

IMPORTANT

Snapchat cannot provide legal advice to law enforcement officials. As such, should you seek further clarification about ECPA's requirements and restrictions on providers like Snapchat, we suggest you contact the Department of Justice's Computer Crime and Intellectual Property Section (CCIPS) at 202-514-1026 and ask to speak to the Duty Attorney.

Snapchat and Law Enforcement

Snapchat is a smart phone application accessed through the iPhone AppStore or Google Play. The application provides a new way to share moments with photos and videos. The purpose of this guide is to familiarize law enforcement agencies with the categories of information available from Snapchat and the specific legal process necessary to obtain that information.

Snapchat is committed to assisting law enforcement investigations to the fullest extent allowed by applicable law. In addition to this guide, Snapchat also provides phone and email support to law enforcement agencies for both emergency and nonemergency inquiries. Contact information for law enforcement support is listed on the cover of this guide.

The primary set of laws governing Snapchat's ability to disclose user information is found in the Electronic Communications Privacy Act, 18 U.S.C. § 2701, et seq. ("ECPA"). ECPA mandates that Snapchat may disclose certain user information to law enforcement only in response to specific types of legal process, including subpoenas, court orders, and search warrants. Generally speaking, ECPA permits the disclosure of basic user identity information, login information, and account content in response to legal process.

Snapchat cannot provide legal advice to law enforcement officials. As such, should you seek further clarification about ECPA's requirements and restrictions on providers like Snapchat, we suggest you contact the Department of Justice's Computer Crime and Intellectual Property Section (CCIPS) at 202-514-1026 and ask to speak to the Duty Attorney.

How Snapchat Works

User takes a photo or video using their camera phone in real-time. The user then selects a preview time of 1-10 seconds for the receiver to view the photo or video. A user can elect to have the photo/video saved in their phone's photo gallery or just sent via Snapchat, without being saved. The photo/video can be sent to a friend in Snapchat or a contact in the user's phone. If the contact in the user's phone does not have Snapchat, the contact must download the application before viewing the photo or video.

Locating a Snapchat Account

Identifying the "Username"

Before sending a legal request to Snapchat you must first identify the username of the account. If you are unable to locate a username, Snapchat can try to locate the account with a phone number or email address.

User Records Maintained by Snapchat and the Process Required to Obtain These Records

Snapchat stores the following information for each user:

- Email
- Phone number
- Username

- A log of the last 200 snaps that have been sent and received (similar to a phone record)
- Date Account was Created Snapchat does not store any image or video data as it is deleted immediately after the recipient views the image or video. If an image or video has not been viewed, it remains on the Snapchat server for 30 days, and then it is removed.

Please note: Snapchat is consistently updating with new features to improve the user's experience and functionality of the site.

In order to release account records on a non-emergency basis, Snapchat requires proper legal process in order to provide records. The required legal process for this information is described below in detail.

In addition to including a Snapchat username, please also indicate if results must be returned before a specific date and where results should be returned. Snapchat accepts service via mail, email and fax and will produce documents in response to out-of-state domestic legal process such as subpoenas, court orders, emergency requests, consent letters, and search warrants.

Process will be accepted by fax (310-943-1793), by email to lawenforcement@snapchat.com, or by mail (at the address on the cover of this Guide).

Subscriber information

Subscriber information is collected when a user creates a new Snapchat account, or alters information at a later date. Please note that not all listed information is required, and that user provided subscriber information is not always independently verified by Snapchat. Subscriber information includes:

- Snapchat Username (user determines)
- Email address
- Phone Number
- Facebook account synced
- Log of the last 200 snaps sent and received (similar to phone record)
- Snapchat account creation date

Process required for subscriber information: subpoena (including grand jury subpoenas), administrative subpoena or civil investigative demand pursuant to 18 U.S.C. § 2703(c)(2); or court order; or search warrant; or user consent.

Preservation Requests

Snapchat honors requests from law enforcement to preserve information in accordance with 18 U.S.C. § 2703(f). Upon receiving a preservation request, Snapchat will preserve all available account information associated with the username listed in the request in an offline file for up to 180 days and will extend the preservation as necessary at your request.

Snapchat will only preserve information for active accounts. If a request to preserve information is received after an account has been deleted, Snapchat is not able to honor the request. If the account is deleted by the user after the receipt of the preservation request, however, all account information present on the date your preservation letter was received will be available upon receipt of proper legal process.

Note Regarding All Legal Requests Following Preservations

When serving follow-up legal process for information that was previously the subject of a preservation request, please specify that the request is seeking both the information preserved and any updated user account information. Please also reference any prior preservation requests by date so that Snapchat may respond to your legal process more efficiently.

Emergency Requests

Under 18 U.S.C. §§ 2702(b)(8) and 2702(c)(4), Snapchat is permitted to disclose information, including email address, phone number, and a log of the last 200 snaps voluntarily when Snapchat believes in good faith that an emergency involving danger of death or serious physical injury to any person requires the immediate discloser of this information.

You may provide a written request for the release of user records on an emergency basis and email (lawenforcement@snapchat.com) or fax the request to 310-943-1793. All emergency requests must be on agency letterhead and/or come from a valid law enforcement email address. A sample Emergency Disclosure form is provided toward the end of this guide. When drafting your emergency disclosure request, please describe the nature of the emergency as specifically as possible and request all information that you require to resolve the emergency situation.

User Consent

Snapchat will disclose information based on user consent obtained by law enforcement where sufficient information is provided to verify that the person providing the consent is the actual creator of the account, and where law enforcement endorses the authenticity of the consent.

A sample consent form is located in Section VIII (d) of this guide. Each consent letter must contain the following information:

- Snapchat Username
- Email address
- Phone Number

Snapchat will not release information if the user is unable or unwilling to provide registration information that correlates to the information on record with Snapchat. In the event that the information provided by the user does not match the information retained by Snapchat, proper legal process will be required before any information is released.

Snapchat Retention Periods

The retention periods identified below reflect Snapchat's retention of user data in the ordinary course of business. Snapchat honors all law enforcement preservation requests made during the period the data is available.

Active Accounts

Subscriber information and account content: The basic identity information entered by a user in creating an account, and all content displayed on the account are maintained as long as the user has not edited the data or removed the content from the account. Once the user makes a change, the previously existing information is overwritten. Upon receipt of a preservation request, however, Snapchat will capture all user data available at that time, and future actions by the user will not affect the preserved data.

Sample Language and Forms

This section provides sample language that law enforcement may use to complete the section of their legal process identifying the information they seek from Snapchat. These are examples of the most commonly requested information from Snapchat. It is important to be as specific as possible when identifying the information you are requesting from Snapchat.

Sample Subpoena Language for Basic Subscriber Information and Snap Logs:

“Records concerning the identity of the user with the Username xxxxxx consisting of: email address, account creation date, and a log of the last 200 snaps sent by account for account accesses.”

Sample Preservation Request Letter

(Must be on the investigative agency or department letterhead)

Dear Custodian of Records:

The below listed account is the subject of an ongoing criminal investigation at this agency, and it is requested pursuant to 18 U.S.C. § 2703(f) that the following information associated with said account be preserved pending the issuance of a search warrant or other legal process seeking disclosure of such information:

[Specify Username to be preserved]

I understand that Snapchat reserves the right to delete any account that violates its Terms of Service.

If you have any questions concerning this request please contact me at *[insert e-mail address and phone contact]*

Thank you for your assistance in this matter.

Sincerely,

(Your Signature)
(Your Name Typed)
(Your Title Typed)

Sample Emergency Disclosure Form

(Must be on the investigating agency or department letterhead)

Dear Custodian of Records:

I request release of records for Username XXXXXX on an emergency basis pursuant to 18 U.S.C. § 2702(b)(7) and § 2702(c).

I have provided below answers to the following questions in enough detail as I am able to in order to provide a good faith basis for release of records on an emergency basis:

- What is the nature of the emergency involving death or serious physical injury?
- Whose death or serious physical injury is threatened?
- What specific information in Snapchat's possession related to the emergency do you need?

Signature of Officer

Printed Name of Law Enforcement Officer

Date

Sample Consent Form

(Must be on the investigating agency or department letterhead)

I, "XYZ", being duly sworn, on this [insert date] do hereby state the following:
I have one or more accounts on Snapchat.com.

- The Usernames are:

  ____

I understand that the "XXXX" agency is conducting an official criminal investigation and has requested that I grant my consent to authorize the "XXXX" agency to access, request, receive, review, copy and otherwise utilize, as they deem appropriate, the following information from the above accounts: [specify information sought]

I hereby authorize Snapchat.com to provide to any agent of the above referenced agency, the above specified information associated with my identified Snapchat.com accounts/accounts.

The following information should be used to verify my identity:

- Email address for account________________________________

- Phone Number for account_______________________________

Pursuant to this Consent, I waive any claims against, indemnify and hold harmless Snapchat.com, its affiliates, and their respective directors, officers, agents, and employees from and against any claims, damages or expenses relating to or arising from, in whole or in part, the disclosure of such information, records and data.

I have not been promised anything in exchange for providing this consent and authorization.

In witness whereof, the undersigned makes the above statements under penalty of perjury.

________________________________ ______________________
Snapchat User Signature Date

____
Printed Name

________________________________ ______________________
Law Enforcement Witness Signature Date

____
Printed name and title

LINKEDIN

Topics Covered

IMPORTANT

This document describes procedures law enforcement authorities should follow to request data from LinkedIn.

What Types of Data Requests Can I Make?

In order to earn and maintain the trust of our Members, LinkedIn strives to ensure that our policies, procedures, and practices provide the clarity, consistency, and control that our Members have come to expect from us. Consistent with this, we respond to law enforcement requests for our Members' data as permitted by our Terms of Service. Thus, we require that law enforcement requests for LinkedIn Member data follow established legal process. We accept only the following types of requests:

- **Data Requests:** A data request is a request for data relating to Member accounts in connection with official criminal investigations. In response to data requests pursuant to formal compulsory legal process issued under U.S. law, we will provide records as required by law. Examples of requests include:
    - Subpoenas
    - Orders issued pursuant to the Electronic Communications Privacy Act
    - Search Warrants
    - Other forms of compulsory process, such as those issued pursuant to Mutual Legal Assistance Treaty (MLAT) with the United States.

- **Preservation Requests:** A preservation request is request top reserve Member account records in connection with official criminal investigations. For requests that identify an account by (1) full name (first and last) and email address associated with the account, or (2) LinkedIn public profile URL (see below for description of exactly what identifying information is required), we will preserve one-time snapshot of then-existing account records for 90 days, pending service of formal legal process. To ensure that all requests are legitimate, we will respond only to requests on law enforcement letterhead that are signed and include a valid return email address. Importantly, any Preservation Request must contain assurances that the requesting authority is taking steps to obtain court order or other legal process for the data that the authority is asking us to preserve.

- **Emergency Requests:** Emergency requests must be made using the attached Emergency Request Form, and will receive response only if LinkedIn believes in good faith that serious bodily harm or the death of person may imminently occur if we do not respond without delay. The Emergency Request Form must be submitted by law enforcement officer and signed under penalty of perjury.

What Contact Information Must I Provide in a Data Request?

To help us ensure that the requests we receive are from legitimate authorities, we require each law enforcement authority making a request to provide the following information to verify the requester's identity and authority to serve legal process:

- Requesting Agency Name
- Requesting Agent Name
- Requesting Agent Badge/Identification Number

- Requesting Agent Employer-Issued E-mail Address
- Requesting Agent Phone Number (including extension)
- Requesting Agent Mailing Address (P.O. Box will not be accepted)
- Requested Response Date (Please allow at least 3 weeks for processing; see below for emergency requests)

What Information Must Be Included in a Data Request?

To ensure that our Members' data remain as private and secure as possible, we scrutinize and evaluate every request for Member data to ensure that they satisfy the applicable legal standards and processes. In this regard, maintaining consistent standards serves two purposes: (1) it ensures that our Members have the clarity, consistency and control over their data that they expect; and (2) it enables us to deal with proper law enforcement requests as promptly and efficiently as possible. Again, detailed information helps us both maintain our Members' trust and ensure that proper requests are dealt with as quickly as possible. Accordingly, LinkedIn requires that all requests provide the following information to identify the individual or account from which information is being sought. Without this information, we will be unable to fulfill your requests:

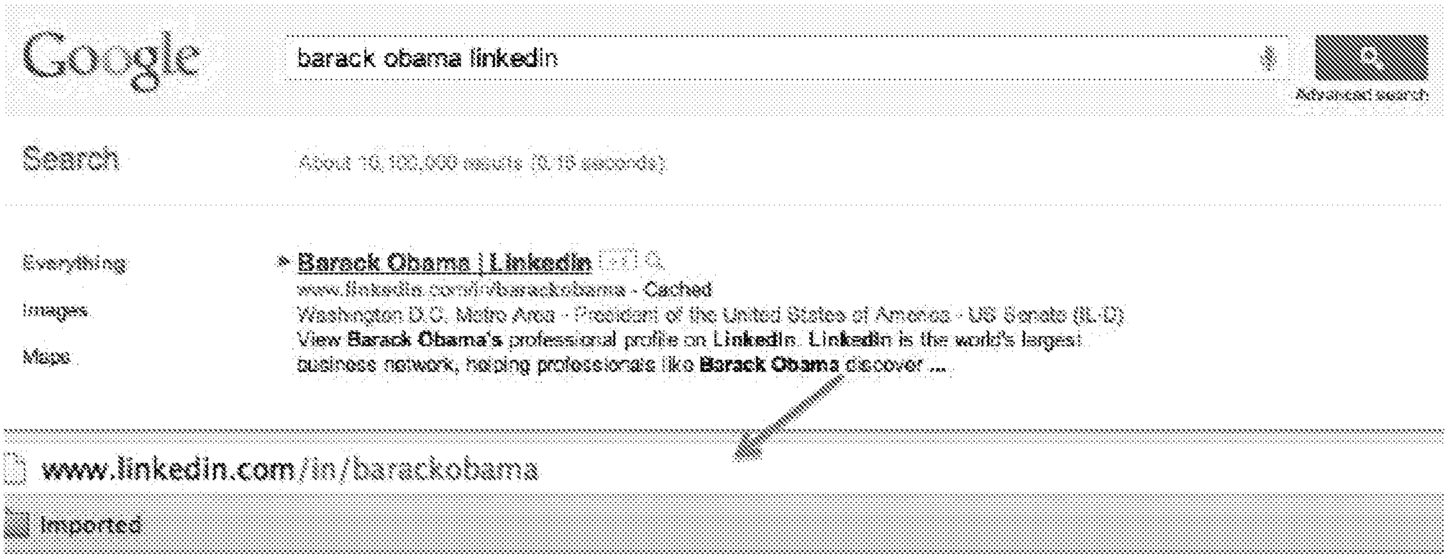
- The full (first and last) name of the LinkedIn Member and email address associated with the account; or,
- The LinkedIn public profile URL.

Please note: LinkedIn public profile URLs come in 2 formats:

- Requesting Agency Name Standard Public Profile URL, for example: http://www.linkedin.com/pub/arnold-bell/37/758/579; and,
- Customized Public Profile URL, for example: http://www.linkedin.com/in/barackobama

How to Find a Subject's Public Profile:

- You may search for the subject's LinkedIn profile via an outside search engine such as Google, Bing,e tc., while NOT logged into your LinkedIn account (for example by searching for "John Doe LinkedIn" via Google). Clicking on the link provided at the outside search engine's site typically directs you to the public profile of the LinkedIn Member, and the public profile URL will appear at the top of your web browser after clicking.

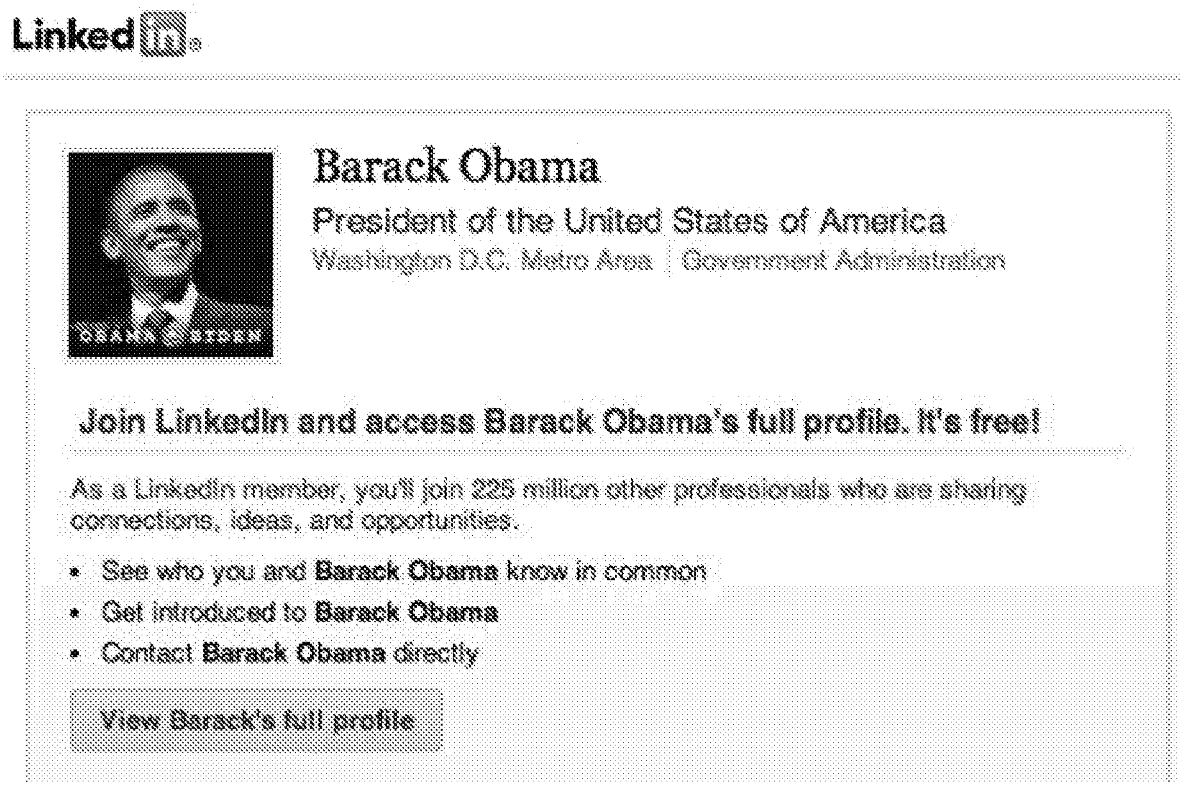


barack obama linkedin

About 10,100,000 results (0.15 seconds)

Barack Obama | LinkedIn
www.linkedin.com/in/barackobama - Cached
Washington D.C. Metro Area - President of the United States of America - US Senate (IL-D)
View Barack Obama's professional profile on LinkedIn. LinkedIn is the world's largest business network, helping professionals like Barack Obama discover ...

www.linkedin.com/in/barackobama



Barack Obama
President of the United States of America
Washington D.C. Metro Area | Government Administration

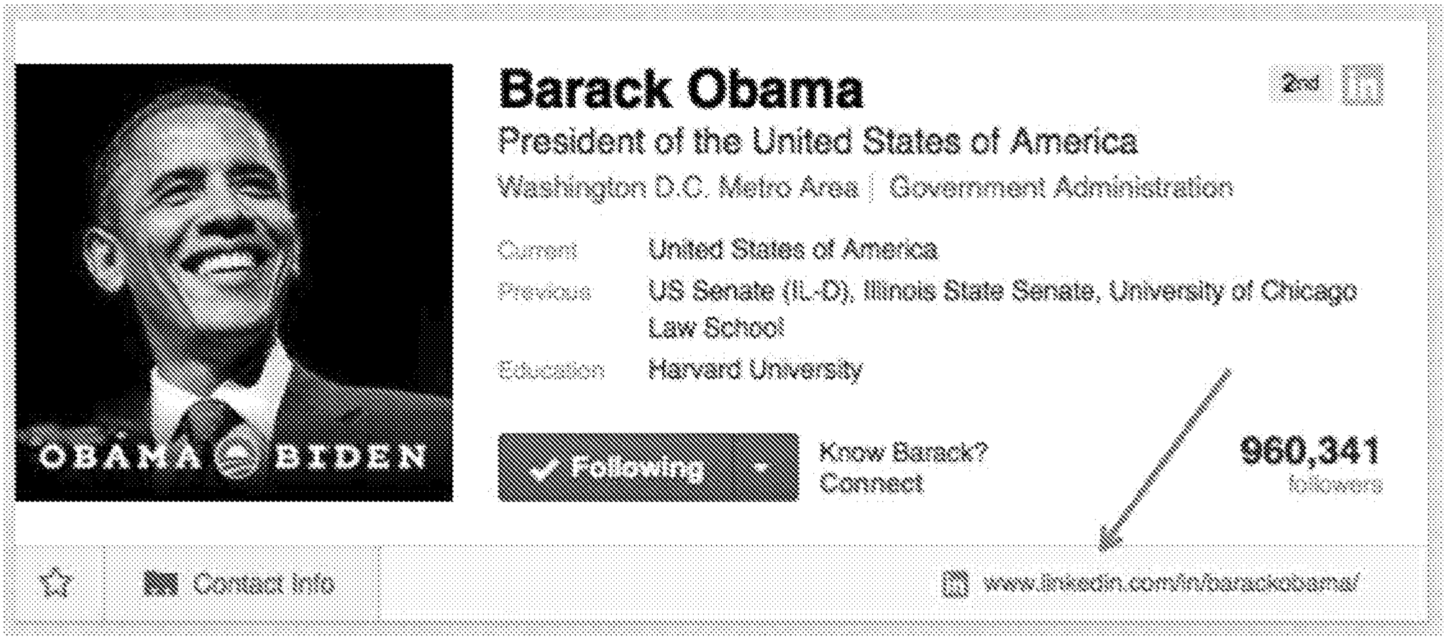
Join LinkedIn and access Barack Obama's full profile. It's free!

As a LinkedIn member, you'll join 225 million other professionals who are sharing connections, ideas, and opportunities.

- See who you and Barack Obama know in common
- Get introduced to Barack Obama
- Contact Barack Obama directly

View Barack's full profile

- Alternatively, if you are logged into your LinkedIn account, you may search for the subject's profile through LinkedIn's search box in the upper right hand corner of the screen. If you are able to locate the subject's profile and can view the subject's profile page, the public profile URL will be identified under the field "Public Profile" at the bottom of the box located near the top of the web page.



Barack Obama

President of the United States of America

Washington D.C. Metro Area | Government Administration

Current	United States of America
Previous	US Senate (IL-D), Illinois State Senate, University of Chicago Law School
Education	Harvard University

www.linkedin.com/in/barackobama/

What Types of Data May Be Available in Response to a Request?

Much of the information on LinkedIn is public – it can be found searching on LinkedIn or even using a search engine such as Google, Bing, etc. However, depending on the type of formal legal process provided, we may be able to respond with one or more of the following types of data:

Basic subscriber information, which may include:

- Email address
- Member Identification number
- Date and time stamp of account creation
- Billing information
- Snapshot of Member Profile Page (see description below)
- IP Logs (see description)

Snapshot of Member Profile Page may include:

- Profile Summary

- Experience
- Education
- Recommendations
- Groups
- Network Update Stream
- User profile photo

Please Note: LinkedIn's commitment to its Members' privacy extends beyond protecting what Membersc hoose to share with our professional community. LinkedIn also respects our Members' choices about what they no longer want to share. Accordingly, LinkedIn does not retain a copy of information from a Member's profile page once the information is revised by the Member. Additionally, if a Member closes his or her account, we delete or de-personalize all information from that account within 30 days.

IP Logs, when available, may include:

- Member ID – the LinkedIn Member ID accessing the account
- IP address – the source IP address
- The date the account was accessed
- Visits – the number of times the linkedin.com website was accessed by that account on the date

Pursuant to a search warrant from an entity with proper jurisdiction over LinkedIn, LinkedIn may also be able to provide Member connections and private communications, which may include (1) Invitations, (2) Messages, and (3) Connections. NOTE, however, that LinkedIn cannot recover the content of Invitations or Messages once they are permanently deleted by the Member, and will not be able to recreate evidence of Connections that have been severed.

LinkedIn strongly believes that all data, whether analog or digital, whether stored on personal computers or in the cloud, is subject to full Fourth Amendment protection, no less than documents stored in file cabinet or in a desk drawer. Thus, given our members' expectations of privacy, we require a search warrant to produce all content, including without limitation, Connections.

Will LinkedIn Notify Members of Requests for Account Data?

Yes. When our Members trust LinkedIn with information about their professional lives, they expect to have control over their data. Thus, LinkedIn's policy is to notify Members of requests for their data **unless it is prohibited from doing so by statute or court order**. Law enforcement officials who believe that notification would jeopardize an investigation should obtain an appropriate court order or other process that specifically precludes Member notification, such as an order issued pursuant to18U.S.C. § 2705(b). Additionally, if your data request draws attention to an ongoing violation of our terms of use, we may, in order to protect the network and other LinkedIn Members, take action to prevent any further abuse, including actions that could notify the Member that we are aware of his or her misconduct.

Are There Any Additional Requirements for Non-U.S. Requests?

Yes, a Mutual Legal Assistance Treaty (MLAT) request or letter rogatory is required for disclosure of information regarding a non-U.S. request.

What Should I Do If I Have an Emergency Request for Data?

As set forth above, LinkedIn takes significant steps to protect its Members' data, including requiring valid legal process before producing any information regarding any of our Members or their accounts. However, we are also aware that certain emergency situations may arise that require the disclosure of Member data. For these purposes, an emergency situation is only one involving imminent serious bodily harm or death. Where these circumstances are present, emergency requests must be made using the attached Emergency Request Form. The Emergency Disclosure Request must be submitted by law enforcement officer and signed under penalty of perjury. LinkedIn will respond to these requests only if it believes in good faith that imminent serious bodily harm or the death of person may occur if we do not respond without delay. In all other cases, LinkedIn will disclose information only pursuant to valid legal process that satisfies the requirements set forth above and all applicable legal standards.

How do I Serve Data Request to LinkedIn?

A data request may be served by fax to 650-810-2897, by certified mail, express courier, or in person at our corporate headquarters at our address set forth below:

LinkedIn Corporation

ATTN: Legal Department

2029 Stierlin Court

Mountain View, CA 94043

USA

EMERGENCY DISCLOSURE REQUEST FORM

Requesting Agency Name:

Requesting Agent Name:

Requesting Agent Badge/Identification Number:

Requesting Agent Employer-Issued E-mail Address:

Requesting Agent Phone Number (including extension or cell phone):

Detailed description of the nature of the emergency and why the threat is imminent (i.e., description of why there is potential for imminent serious bodily harm or death and why the normal disclosure process would be insufficient):

Identifying Information for Member account ((1) LinkedIn public profile URL or (2) name and email address):
Detailed explanation of information needed to resolve emergency (Please do not respond by asking for all available information as this will likely result in delaying or denying your request):

I declare, under penalty of perjury, that to the best of my knowledge, the foregoing is true and correct.

Signature and Badge Number

Date

Name

Social Media for Law Enforcement: Friend or Foe

This course familiarizes investigators with some of the social media tools available to them throughout an investigation. Key topics covered in this course are: how to search for individual accounts using [redacted] and how to find useful public content on social media sites for investigations.

b7E

Table of Contents

Getting Started

What will this course cover?

Welcome to “Social Media: Friend or Foe”

This course familiarizes investigators with some of the social media tools available to them throughout an investigation. Key topics covered in this course are: how to search for individual accounts using [redacted]; how to find [redacted] and how to find useful public content on social media sites for investigations. b7E

Why is this course important to investigators?

There is a substantial amount of valuable information available through social media, but you would have to know where to go and how to search for it. By applying the techniques and by using the tools presented in this course, you will gain yet another path of useful leads in an investigation.

Scenario Description

This course places you in an interactive environment in which you will receive immediate feedback based on the choices you make throughout the course to solve the given case. Every module will introduce new material and provide an update on the current phase of the investigation. At the end of each module, you will use the given information to contribute in each step of the investigation until in the end the case is solved!

Course Instructional Goal and Learning Objectives

The goal of this course is to illustrate how investigators can utilize social media, consistent with policy, to further their investigations.

After completing this course, investigators will be able to:

1. Explain the unique advantages of using different social media sites [redacted] b7E
2. Perform [redacted] for investigative purposes on social media sites [redacted]
3. Explain proper procedures for conducting social media searches

DISCLAIMER

This course features a job aid that includes social media sites investigators can use consistent with policy to help with their investigations. However, the sites introduced in this course are not all-inclusive. Please note there are many more available through the internet.

IMPORTANT: Please remember the sensitivity and legal requirements of using social media. Please contact your state or local prosecuting attorney for further guidance.

About this Course

This course is divided into three lessons, each one gets you a step closer to solving the case, and concludes with a summary:

- Lesson 1: What's In a Username
- Lesson 2: Strategic Social Searches
- Lesson 3: Tale-telling [redacted] b7E

This course is designed to encourage the use of the job aids to complete some of the learning activities. There are two job aids in this course: Social Media Guidelines for Law Enforcement and Social Sites Capabilities, which are also available as stand-alone references located in the Appendix.

As your investigation unfolds, any helpful facts that you find will be added to your investigative notes.

Lesson 1: What's In a Username

Introduction

This lesson will introduce you to the case you will be investigating during the course. You will learn about the information already gathered and the investigative work already conducted.

You will be introduced to [redacted] a couple of tools that can be more useful than Google or Bing when searching social media sites. b7E

After completing this lesson, you will be able to:

- Perform a search on [redacted]
- Explain the advantages of using [redacted] over Google or Bing
- Identify the benefits of using [redacted]

IMPORTANT NOTICE

This investigation is fictitious in nature and is not designed to teach investigative strategies. The purpose of this course is to provide an interactive and stimulating vehicle to raise an awareness of social media sites and their potential benefits in an investigation.

FYI –[redacted]

b7E

[redacted]

Deep Web refers to a vast repository of underlying content, such as documents in online databases that general-purpose web crawlers cannot reach. The deep web content is estimated at 500 times that of the surface web, yet has remained mostly untapped due to the limitations of traditional search engines. Any documents or information found through the deep web will still require investigators to contact the companies in possession of the information and present the required legal documents to access the information.[redacted] [redacted]

[redacted]

b7E

[redacted]

Conclusion

This lesson introduced you to the case you will be investigating during the course. You learned about the information already gathered and to the investigative work already conducted.

You were introduced to [redacted] a tool that is more useful than Google or Bing when searching social media sites. b7E

Now that you have completed this lesson, you should be able to:

- Perform a search on [redacted]
- Explain the advantages of using [redacted] over Google or Bing
- Identify the benefits of using [redacted]

Lesson 2: Strategic Social Searches

Introduction

This lesson explores the steps that you would need to perform searches on [redacted] and to search [redacted]

b7E

After completing this lesson, you will be able to:

- Perform searches on [redacted]
- View and interpret results displayed on [redacted]
- Use a [redacted]
- Navigate through [redacted]

[redacted]

b7E

FYI – Using Social Sites

When it comes to social sites, despite an individual's efforts to keep their information private, [redacted]

b7E

Conclusion

This lesson explored the steps that you would need to perform searches on [redacted] and to search [redacted]

b7E

Now that you've completed this lesson you:

- Performed searches on [redacted]
- Viewed and interpreted results displayed on [redacted]
- Used a [redacted]
- Navigated through [redacted]

Lesson 3: Tale-telling [redacted]

b7E

Introduction

This lesson introduces [redacted] which allows you to search for and view [redacted] based on the given parameters. You will explore the steps needed to perform [redacted] [redacted]

After completing this lesson, you will be able to:

- Perform [redacted]
- Obtain [redacted] relevant to keywords
- Refine searches on [redacted]

FYI – Twitter

Twitter's is a real-time information network that lets users share and discover what's happening now. Law enforcement must provide Twitter a subpoena for subscriber information.

Emergency Situations: These require an emergency disclosure request to obtain this information more quickly.

Covert Operations: It's important to note that most service providers have a policy to notify subscribers when law enforcement serves process for any information. In case of a covert investigation, you must submit a court order for non-disclosure along with a subpoena.

Following a Feed: Joining an e-mail list or a Twitter feed of an organization is participation that must abide by the policy of your organization. If the general public is not able to sing up to the twitter feed or the email list, then additional approvals may be necessary.

Most Twitter profile information is public, so anyone can see it. A Twitter profile contains a profile photo, header photo, background image, and status updates, called tweets. In addition, the user has the option to fill out location, a URL, and a short "bio" section about themselves for display on their public profile.

[redacted]

b7E

Remember!

Twitter Search can be used to identify tweets containing a word or phrase within a geographic location. These tweets can be helpful to investigators using Twiitter to create a stream of relevant information. [redacted] Also remember that only those Tweets that are pertinent to and within the scope of the case may be collected.

b7E

Conclusion

This lesson introduced [redacted] which allows you to search for and view [redacted] based on the given parameters. You explored the steps needed to perform [redacted]

b7E

Now that you've completed this lesson, you've:

- Performed [redacted]
- Obtained [redacted] relevant to keywords
- Refined searches on [redacted]

Course Summary

What did this course cover?

This course explored social media tools available to you throughout an investigation. Through the scenario, you learned how to continue a search after hitting road-blocks using common search engines such as Google or Bing; how to find [redacted] and how to find useful information through content that subjects post and make public on social media sites. b7E

Now that you've completed this course, you should be able to:

1. Explain the unique advantages of using different social media sites [redacted]
2. Perform [redacted] for investigative purposes on social media sites [redacted]
3. Explain proper procedures for conducting social media searches

More Investigative Technology Courses and FYIs

- *Basic Networking for Law Enforcement*
- *Exploiting Mobile Communications for Law Enforcement: Criminal Tactics and Investigative Techniques*
- *Obtaining and Analyzing Digital Records for Local law Enforcement*
- *The Cloud for Local Law Enforcement: It's all about Communication*
- *Investigating Websites for Law Inforcement: A Wealth of Information*
- *Tracing Email Addresses for Law Enforcement*
- *FYI: Email Draft Folder Messaging Podcast*
- *FYI: File Hashing*
- *FYI: Using Public Records Databases in Investigations*
- *FYI: Virtual Worlds*

Still have questions?

If you need more in-depth expertise on this topic, please contact technical experts in your area.